Notre vie privée est-elle réellement mise en danger par les robots ?

Delforge, Antoine; Gerard, Loïck

Published in:
Intelligence artificielle et droit

Publication date:
2017

Document Version
le PDF de l'éditeur

TITRE 2
Notre vie privée est-elle *réellement* mise en danger par les robots ? Étude des risques et analyse des solutions apportées par le GDPR

Antoine DELFORGE[*] et Loïck GÉRARD[**]

Introduction

Alors que les divergences sont nombreuses en ce qui concerne la définition même de ce qu'est un robot, il est au moins un point qui ne semble guère faire controverse : les robots – quels que soient leurs fonctions et leurs formes – disposent de la capacité de percevoir et d'enregistrer leur environnement et ont par conséquent la capacité de collecter des données en grand nombre, ce qui peut porter atteinte à la vie privée de leurs utilisateurs et des tiers[1].

Avant de procéder à l'analyse de la règlementation applicable à la protection des données à caractère personnel, il nous semble opportun d'effectuer une analyse des atteintes que ces objets encore largement méconnus peuvent causer au droit à la vie privée.

En tout état de cause, les robots, aussi bien physiques que virtuels, représentent un nouveau défi pour les législateurs et les outils de protection de la vie privée que ceux-ci ont progressivement mis en place. En effet, l'émergence des robots lève le voile sur de nouvelles problématiques ou, à tout le moins, vient amplifier des inquiétudes préexistantes quant à la

[*] Chercheur à l'Université de Namur (CRIDS).

[**] Assistant à l'Université de Namur (CRIDS). Les auteurs tiennent à remercier Karen Rosier pour sa relecture attentive et ses précieux conseils.

[1] C. HOLDER, V. KHURANA, F. HARRISON et L. JACOBS, « Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II) », *Computer Law & Security review*, n° 32, 2016, p. 391.

protection de la vie privée et des données à caractère personnel générées par les utilisateurs.

En prenant le recul nécessaire, il apparaît cependant que la question des atteintes à la vie privée causées par les robots renvoie à celle, plus large, de la manière dont les technologies émergentes viennent repousser les limites du raisonnement juridique et de l'interprétation des textes de loi. Les exemples de ce type de phénomène sont légions : le secret des lettres reconnu par l'article 29 de la Constitution peut-il être invoqué s'agissant de courriers électroniques[2] ? Le 4e Amendement de la Constitution américaine exige-t-il qu'un mandat de perquisition soit délivré pour procéder à une écoute téléphonique[3] ? Bien souvent imprévues – car imprévisibles – au moment de l'édiction des normes, ces questionnements sont alors destinés à être résolus par l'intermédiaire de l'interprétation des cours et tribunaux.

CHAPITRE 1. Les robots : source de risques pour la vie privée ?

1. Structure du chapitre – Au moins six risques potentiels liés aux robots et à leur développement peuvent être identifiés : le risque de surveillance accrue (section 1), d'accès aux endroits « protégés » (section 2), de collecte invisible et permanente (section 3), de cybersécurité insuffisante (section 4), de transfert émotionnel au profit du robot (section 5) et de manque de connaissance des utilisateurs (section 6). Il est à noter que ces risques ne sont pas exclusifs l'un de l'autre et ont au contraire tendance à se renforcer mutuellement.

[2] *Doc. parl.*, Sén., sess. ord. 2014-2015, n° 6-129/1 ; Cass., 21 octobre 2009, R.G. n° P. 09.0766.F.

[3] Telle était la question posée en 1928 à la Cour Suprême dans l'affaire *Olmstead v. United States*. Le raisonnement de la Cour fut le suivant : étant donné qu'aucune intrusion dans le domicile (*physical trespass*) ou saisie de documents (*seizure of materiel tangible effects*) n'avait eu lieu, la protection du 4e Amendement n'était pas applicable. Dans une opinion dissidente, le juge Brandeis considéra toutefois que le 4e Amendement protégeait la vie privée au sens large. Loin de se limiter aux intrusions physiques et la saisie de documents dans le domicile de l'accusé, la portée du 4e Amendement devait être interprété de manière extensive (N. M. Richards et W. D. Smart, « How should the law think about robots ? », *Robot Law* (R. Calo, A. M. Froomkin et I. Kerr dir.), Cheltenham, Edward Elgar, 2016, pp. 13-15).

SECTION 1. – Une surveillance accrue

2. Surveillance directe – L'atteinte potentielle à la vie privée qui vient sans doute en premier à l'esprit lorsque l'on pense aux robots est liée à leur utilisation en tant que moyens de surveillance. Comme le souligne R. Calo, la surveillance directe – c'est-à-dire la surveillance exercée de manière délibérée et volontaire – est grandement facilitée par les développements de la robotique[4]. Sans rentrer dans de grandes explications techniques, il apparaît évident que les robots renforcent la capacité de l'homme à surveiller son environnement : les robots ont accès à des endroits et points de vue inaccessibles aux humains[5] et les performances de leurs capteurs en font de bien meilleurs observateurs que nous ne le sommes. En outre, la variété des formes qu'ils peuvent prendre, la diversité des lieux et environnements dans lesquels ils peuvent opérer, ainsi que leur potentielle petite taille – à même de les rendre quasi invisibles à l'œil d'une personne non-avertie – en font des moyens de surveillance bien plus polyvalents et moins ostensibles que le sont de « simples » caméras de surveillance fixes ou des agents de surveillance.

Le problème posé par cette augmentation des capacités de surveillance semble relativement évident : plus les personnes sont surveillées, moins la sphère de leur vie privée est importante. Il est toutefois un risque plus insidieux lié aux capacités de surveillance rendues disponibles par les robots. Ce risque tient à la perception et à la réalité de la surveillance dont les personnes font l'objet.

3. Sentiment de surveillance – Comme le met en évidence D. J. Solove, l'incertitude quant à l'existence ou non d'une surveillance de nos actes et comportements peut être comprise en faisant référence au roman 1984 de George Orwell et à la surveillance mise en place par le gouvernement autoritaire *Big Brother*[6]. Dans le monde décrit dans l'œuvre, le gouvernement assoit son pouvoir en utilisant tous les moyens disponibles pour éradiquer la vie privée de ses citoyens. L'outil principal utilisé par *Big Brother*

[4] R. Calo, « Robots and Privacy », *Robot Ethics: The Ethical and Social Implications of Robotics* (P. Lin, G. A. Bekey et K. Abney dir.), Cambridge, MIT Press, 2012, p. 187.

[5] On pense, évidemment, aux drones mais également aux micro- et nanorobots tels les « insectes robotiques » développés par le DARPA (*Defense Advanced Research Projects Agency*, agence étatique sous l'autorité du département de la Défense des États-Unis) dont les recherches se focalisent désormais sur la création de « robots-mouche » capables d'atteindre leur lieu de surveillance via des espaces étroits (G. Sheftick, *Army developing robotic insects ?*, 16 décembre 2014, dispo. sur : https://www.army.mil/article/140097).

[6] D. J. Solove, *The Digital Person : Technology and Privacy in the Information Age*, New-York, New York University Press, 2004, pp. 29-35.

est le télécran, dont l'installation est obligatoire dans chaque habitation. Le télécran est inspiré des écrans de télévision ordinaires dont il reprend l'aspect et la fonctionnalité principale. Toutefois, il a pour particularité de fonctionner sur le principe du miroir sans tain. De la sorte, il permet à *Big Brother* d'observer les personnes qui se trouvent en face du télécran sans que celles-ci soient en mesure de déterminer si elles sont ou non observées à un moment précis.

Partant de cette métaphore, la démonstration peut être faite qu'au-delà d'une surveillance réelle, la simple impression – voire la simple suspicion – quant à la possibilité de faire l'objet d'une écoute ou d'un enregistrement peut suffire à provoquer une forme de retenue de la part des personnes. Cette retenue peut s'interpréter comme une renonciation ténue mais bien réelle au plein et entier exercice de son droit à la vie privée[7]. Il en va par exemple ainsi de la personne qui, de peur d'être enregistrée, se contraint à une forme d'autocensure en restreignant sa prise de parole et l'expression de ses convictions[8]. Il en va de même pour la personne qui, ne sachant pas si ses gestes sont observés, renonce à adopter un comportement considéré comme excentrique, marginal ou jugé tabou par son entourage[9].

Ces risques ne sont pas inhérents aux robots et préexistent au développement de ceux-ci. Toutefois, la prolifération des robots, leurs capacités d'enregistrement et leur aptitude à la discrétion constitue un risque réel. Ce risque est que le sentiment de surveillance – que celle-ci soit réelle, supposée ou tout simplement imaginée – se trouve encore renforcé. Pour le formuler autrement, le risque est que la surveillance devienne « permanente dans ses effets, même si discontinue dans son action »[10] et entraine un réel recul dans l'exercice des droits.

[7] Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 juillet 2002, req. n° 2346/02, § 61 ; C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *Proceedings of the 2015 ACM Websience Conference*, New-York, ACM, 2015, p. 3.

[8] Sur ce sujet, voy. E. Stoycheff, « Under Surveillance : Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », *Journalism & Mass Communication Quarterly*, vol. 93, 2016, pp. 296-311.

[9] J. E. Cohen, « Examined Lives : Informational Privacy and the Subject as Object », *Stanford Law Review*, vol. 52, 2000, p. 1426 cité par D. J. Solove, *The Digital Person : Technology and Privacy in the Information Age*, *op. cit.*, p. 176.

[10] M. Foucault, *Surveiller et punir*, Paris, Gallimard, 1975.

SECTION 2. – Un accès à des endroits jusqu'alors « protégés »

4. Présence consentie – Comme cela a été précisé, la variété dans les formes, les capacités et les tailles des robots fait que ceux-ci sont susceptibles d'avoir accès – avec ou sans consentement préalable – à des espaces jusqu'ici considérés comme relativement étanches à toute forme de surveillance.

En outre, l'accès à des lieux fondamentalement privés peut également être intrinsèquement lié aux fonctions pour lesquelles le robot a été conçu et mis sur le marché. Tel est par exemple le cas de la robotique de service et des robots compagnons destinés à devenir les « assistants domestiques » de leur propriétaire.

Contrairement à la problématique précédente relative à la surveillance active par le biais de robots imaginés et conçus dans cette optique, la présence de robots de service auprès de leurs utilisateurs ne paraît pas soulever de grandes questions relatives au droit à la vie privée. En effet, on se trouve ici face à un robot dont la présence a été souhaitée par son utilisateur et dont l'intrusion dans la vie privée de celui-ci a vraisemblablement été consentie[11].

5. Présence constante – C'est toutefois dans la vocation même des robots de service que se trouve le risque pour la vie privée de leurs utilisateurs. L'essence même du robot de service est d'assister son utilisateur dans l'accomplissement des tâches quotidiennes de celui-ci. Comme le précise O. Guilhem, directeur juridique d'Aldebaran Robotics, ces robots « sont polyvalents et offrent une multitude de services : répondre à vos questions, raconter une histoire à vos enfants, rappeler les médicaments à prendre aux personnes âgées, [...] faciliter l'échange avec des enfants autistes, assurer la surveillance de la maison, tenir compagnie, etc. »[12].

Plus encore, la lecture du déroulement d'une journée-type du robot d'assistance Romeo – développé par Softbank Robotics/Aldebaran – laisse entrevoir l'ampleur de la présence du robot auprès de la personne assistée[13]. Ainsi, nous apprenons que le robot est par défaut en mode « écoute

[11] Que ce consentement ait été donné au moment de l'achat du robot par un particulier ou, par exemple, de l'admission d'une personne au sein d'un établissement de soin ayant recours aux services de robots.

[12] O. Guilhem, « Pour une robotique humanoïde responsable », *Expertises*, 2015, p. 294.

[13] Le « projet Romeo » vise à concevoir un robot capable d'assister une personne en perte d'autonomie. Une phase d'évaluation sera organisée dans un appartement d'un centre de rééducation et consistera « à laisser un robot à la disposition d'une personne âgée pendant une semaine » (https://projetromeo.com/).

et service » ce qui lui permet d'attendre et d'écouter les demandes de l'utilisateur afin de lui porter assistance. En outre, le robot est capable de déclencher certaines actions en fonction de son environnement et des moments de la journée. Ainsi, Romeo peut détecter que son utilisateur est éveillé et déclencher une « routine du matin ». Romeo peut également détecter le sommeil de son utilisateur ; le robot passe alors en mode veille – un mode dans lequel il ne peut pas se déplacer ni faire de bruit – jusqu'au réveil de son utilisateur ou, si celui-ci dort plus longtemps qu'il n'a l'habitude de le faire, jusqu'au moment où le robot prend la décision de venir le réveiller.

On le voit, le robot de service est appelé à être constamment présent aux côtés de son utilisateur, à tout le moins lorsque celui-ci se trouve à son domicile. C'est en cela que le robot de service peut porter atteinte à la vie privée[14].

La présence du robot et – rappelons-le – de ses capteurs au sein du domicile représente un risque pour la vie privée en ce que le robot obtient ainsi accès à des pans de vie qui étaient jusqu'ici considérés comme inviolables car se déroulant dans la stricte intimité du domicile[15]. Ainsi, que penser du robot qui, parce que cela fait partie de ses missions, pénètre dans la chambre de son utilisateur endormi afin d'acquérir des données sur celui-ci et son environnement[16] ?

SECTION 3. – Une collecte invisible et permanente

6. Présence invisible – Étant des objets sociaux – en ce que leur existence implique des activités relationnelles avec leurs utilisateurs – les robots et en particulier les robots d'assistance sont appelés à se fondre

[14] Dans un tel contexte, il convient de s'interroger sur la persistance de l'effectivité du droit d'être laissé seul (« *the right to be let alone* »), considéré comme socle fondamental de la notion de vie privée (S. Warren et L. Brandeis, « The Right to Privacy », *Harvard Law Review*, vol. 4, 1890, pp. 193-220, dispo. sur : http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html). Voy. égal. dans la jurisprudence de la Cour européenne des droits de l'homme : Cour eur. D.H., arrêt *Dudgeon c. Royaume-Uni*, 22 octobre 1981, req. n° 7525/76, opinion partiellement dissidente du juge Walsh, §§ 8-9 ; Cour eur. D.H., arrêt *Malone c. Royaume-Uni*, 2 août 1984, req. n° 8691/79, opinion concordante du juge Pettiti ; Cour eur. D.H., arrêt *Von Hannover c. Allemagne*, 24 juin 2004, req. n° 59320/00, opinion concordante du juge Zupancic ; Cour eur. D.H., arrêt *Delfi AS c. Estonie*, 16 juin 2015, req. n° 64569/09, opinion concordante du juge Zupancic.

[15] R. Calo, « Robots and Privacy », *op. cit.*, p. 192.

[16] C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *op. cit.*, p. 4 ; C. Holder, V. Khurana, F. Harrison et L. Jacobs, « Robotics and law: Key legal and regulatory implications of the robotics age (Part I of II) », *op. cit.*, p. 393.

dans notre environnement. Par accoutumance, le robot fera petit à petit partie des éléments habituels du quotidien auxquels on ne porte plus une attention particulière.

Cette capacité qu'ont les robots à devenir des éléments banals de notre environnement est de nature à les rendre plus dangereux pour la vie privée des utilisateurs car ceux-ci ne les perçoivent plus comme un outil de collecte de données à caractère personnel. Il y a donc une différence entre la collecte réelle de données qui est faite par le robot et la perception de celle-ci par les utilisateurs. La même remarque peut, de manière plus générale, être formulée à l'encontre des objets connectés, des sites Internet ou des applications mobiles. Le fait que ces technologies sont désormais incorporées à nos vies quotidiennes a pour conséquence de rendre la collecte de données quasi invisible à nos yeux. Comme l'a écrit Weiser : « *The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it* »[17].

7. Activité permanente – Toutefois, il est une caractéristique des robots – et de la robotique de service en particulier – qui les différencie des moyens de collecte de données auxquels nous sommes actuellement accoutumés. Contrairement à l'ordinateur ou au téléphone qui nous permet d'accéder à Internet ou à nos applications, le robot de service n'a pas vocation à être éteint. Reprenons l'exemple de Romeo. Nous l'avons vu, celui-ci se met en mode veille lorsqu'il détecte que son utilisateur dort. Il s'agit bien d'un mode veille, non d'une extinction totale. Une partie au moins des senseurs de Romeo restent donc actifs en permanence. En outre, le fait d'éteindre Romeo serait contre-productif : quelle serait la plus-value apportée par un robot d'assistance qui doit être éteint et rallumé « manuellement » ? Cette permanence dans l'activité – même réduite – du robot va de pair avec une permanence dans la collecte de données et le différencie fondamentalement des outils évoqués précédemment.

En outre, le simple fait qu'un consentement a été obtenu avant toute collecte de données à caractère personnel ne suffit pas à s'assurer que l'auteur du consentement est pleinement conscient du fait que ses données vont être collectées et stockées[18]. Comme le soulignent C. Lutz et A. Tamo, les (futurs) utilisateurs de robots ont d'ores et déjà l'habitude de consentir au traitement de leurs données que ce soit en acceptant des conditions générales d'utilisation, en acceptant les cookies sur une page internet, en

[17] Traduction libre « Les technologies les plus envahissantes sont celles qui disparaissent. Elles se fondent dans notre quotidien jusqu'à en faire partie intégrante ». M. Weiser, « The Computer for the 21st Century », *Scientific American*, september 1991, p. 94.

[18] Sur les conditions pour qu'un consentement soit légalement considéré comme valable, voy. *infra*, n° 46.

téléchargeant un logiciel, ou encore en autorisant une application mobile à accéder à leur localisation, leurs photos et leur carnet d'adresses, ...[19] Notre habitude au consentement rend celui-ci automatique et invite à se poser la question de la réelle utilité du consentement en tant que moyen de renoncement partiel au droit à la vie privée[20].

SECTION 4. – Une collecte accrue

8. Données sensibles – Comme cela a été mentionné dans les sections précédentes, les robots – en particuliers les robots de service – ont pour vocation de suivre et d'accompagner les activités de leurs utilisateurs. En outre, ils ont accès aux mêmes lieux que les utilisateurs ce qui revient à dire qu'ils ont potentiellement accès à l'ensemble du domicile. Cet accès global au lieu de vie de l'utilisateur permet au robot de collecter une grande quantité mais également une grande variété de données, dont des données dites sensibles.

On pense en particulier aux données relatives à la santé[21] mais également aux pratiques et préférences sexuelles de l'utilisateur[22]. Il n'est pas non plus exclu qu'un robot d'assistance soit amené à collecter d'autres catégories de données sensibles au cours d'une interaction avec son utilisateur[23]. Prenons à nouveau l'exemple de Romeo. La fiche de présentation du projet précise que le robot peut, sur demande ou d'initiative, poser des questions à son utilisateur. Bien que les exemples donnés (« Quel a été ton plus beau voyage ? », « Quel métier as-tu exercé ? », « Quel est ton plus beau souvenir avec ta meilleure copine ? », ...[24]) semblent relativement anodins, on ne peut exclure que l'utilisateur en vienne – comme lors d'une discussion d'humain à humain – à se laisser emporter par la conversation et à aborder des sujets tels que la politique, la religion, ... Autant de données personnelles sensibles qui pourraient être collectées

[19] C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *op. cit.*, p. 3.

[20] Sur ce point, voy. D. J. Solove, « Privacy Self-Management and the Consent Dilemma », *Harvard Law Review*, vol. 126, 2013, pp. 1880-1903, spéc. pp. 1894-1895.

[21] Cour eur. D.H., arrêt *L.L. c. France*, 10 octobre 2006, req. n° 7508/02 ; Cour eur. D.H., arrêt *I c. Finlande*, 17 octobre 2008, req. n° 20511/03.

[22] Cour eur. D.H., arrêt *Pretty c. Royaume-Uni*, 29 juillet 2002, req. n° 2346/02, § 61 ; Cour eur. D.H., arrêt *S. et Marper c. Royaume-Uni*, 4 décembre 2008, req. n^{os} 30562/04 et 30566/04, § 66 et les références citées.

[23] Pour traiter pareilles données, il est en principe nécessaire de demander le consentement explicite de la personne concernée, voy. *infra*, n° 45.

[24] Voy. https://projetromeo.com/scenario/

par Romeo alors même que ce n'est pas le robot qui a initié ou orienté la conversation sur ces sujets.

9. Capteurs – Qui plus est, les robots sont équipés d'outils de collecte de données d'une grande variété.

Ainsi, une voiture autonome est équipée de caméras, de radars, de sonars, de lidars, de scanners et également d'émetteurs-récepteurs GPS. Ces outils servent évidemment à collecter les informations nécessaires à l'analyse de l'environnement dans lequel le véhicule se déplace mais servent également à collecter des données relatives aux occupants du véhicule : niveau d'attention du « conducteur », rythme cardiaque, émotions, habitudes de conduite, destinations fréquentes, nombre de passagers dans le véhicule, ... Il en va *a fortiori* de même pour le robot d'assistance qui, pour assumer ses fonctions, est amené à collecter des données variées sur la personne assistée.

10. Volume de données – La combinaison de ces deux facteurs – le suivi quasi-constant de l'utilisateur et la variété des données qui peuvent être collectées distinguent les robots des autres moyens de traitement de données et expliquent la grande quantité de données collectées et traitées. À ce titre, l'éditorial publié par le PDG d'Intel le 15 novembre 2016 donne une idée de l'ampleur de la collecte effectuée par un véhicule autonome. On y apprend qu'en 2016, une personne générait approximativement 650 mégabytes de données par jour via l'utilisation de son ordinateur, de son téléphone portable, et d'objets connectés. Par comparaison, une voiture connectée entièrement fonctionnelle est amenée à générer 4000 gigabytes de données par jour, soit environ 6000 fois plus[25].

SECTION 5. – Une sécurité défaillante

11. Cybersécurité – La vie privée des utilisateurs peut également être mise à mal en raison de défaillances dans la cybersécurité des robots[26]. Ainsi, il n'est pas à exclure qu'un tiers puisse prendre le contrôle direct du robot ou intercepter les données que celui-ci envoie et reçoit[27].

[25] B. Krzanich, *Data is the new oil in the future of automated driving*, 15 novembre 2016, dispo. sur : https://newsroom.intel.com/editorials/krzanich-the-future-of-automated-driving/

[26] Voy. Cour eur. D.H., arrêt *Z. c. Finlande*, 25 février 1997, req. n° 22009/93, §§ 95-96 ; Cour eur. D.H., arrêt *I c. Finlande*, 17 octobre 2008, req. n° 20511/03.

[27] Sur les différents types de cyberattaques pouvant être dirigées contre les robots, voy. I. Priyadarshini, « Cyber Security Risks in Robotics », *Detecting and Mitigating Robotic*

Dès 2009, une étude de l'Université de Washington mettait en avant les failles de sécurité présentée par trois modèles populaires de robots[28]. Après avoir testé la sécurité des trois modèles, les chercheurs arrivèrent à la conclusion qu'aucun des robots n'était parfaitement sécurisé. Ainsi, plusieurs failles majeures avaient pu être exploitées :

- premièrement, les robots étaient facilement détectables en ce qu'ils utilisaient un SSID[29] ou une adresse MAC[30] aisément reconnaissable ;
- deuxièmement, les robots se montraient particulièrement sensibles aux risques de mise sur écoute. Faute de cryptage suffisant, les chercheurs ont pu récupérer les identifiants utilisés par les utilisateurs pour se connecter au robot et intercepter les flux audio et vidéo transmis à l'utilisateur ;
- enfin, les chercheurs sont parvenus à prendre le contrôle direct des robots étudiés. Bien que la prise de contrôle des robots était soumise à l'introduction d'un identifiant et d'un mot de passe, ceux-ci avaient été obtenus grâce à une « mise sur écoute préalable ». Une fois les données d'identifications obtenues, les robots étaient – selon leurs spécificités techniques – contrôlables via Internet ou via connexion sur le réseau sans fil auquel ils étaient connectés[31].

Au terme de cette étude, il apparaît clairement que les vulnérabilités des robots proviennent de la faible sécurité de leur connexion avec le réseau et les utilisateurs. Un tel constat attire d'autant plus l'attention que, depuis 2009, la connexion des robots vers l'extérieur s'est fortement développée. En effet, le traitement des informations pour les robots prend de plus en

Cyber Security Risks (R. KUMAR, P. K. PATTNAIK et P. PANDEY dir.), Hershey, IGI Global, 2017, pp. 333-348 ; T. BONACI, J. HERRON, T. YUSUF, J. YAN, T. KOHNO et H. J. CHIZECK, « To Make A Robot Secure : An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics », 2015, dispo. sur : http://brl.ee.washington.edu/teleoperationz/teleoperation-security/.

[28] T. DENNINGS, C. MATUSZK, K. KOSCHER, J. R. SMITH et T. KOHNO, « A Spotlight on Security and Privacy Risks with Future Household Robots : Attacks and Lessons », *Proceedings of the 11th International Conference on Ubiquitous Computing (UbiComp '09)*, New-York, ACM, 2009.

[29] Le SSID ou Service Set Identifier est le nom donné à un réseau sans fil. Les robots expérimentés dans l'étude généraient par défaut leur propre réseau sans fil auquel les utilisateurs pouvaient connecter leurs autres objets.

[30] L'adresse MAC, pour Media Access Control, est un identifiant physique unique propre à chaque carte réseau. Ainsi, chaque robot connecté dispose d'une adresse MAC unique. L'adresse MAC a été utilisée par les chercheurs pour détecter les robots qui ne généraient pas leur propre réseau mais se connectaient à un réseau préexistant (par exemple le routeur installé dans le domicile).

[31] T. DENNINGS, C. MATUSZK, K. KOSCHER, J. R. SMITH et T. KOHNO, « A Spotlight on Security and Privacy Risks with Future Household Robots : Attacks and Lessons », *op. cit.*, pp. 2-4.

plus appui sur les possibilités offertes par le *cloud computing*. De la sorte, les données collectées par les senseurs du robot ne sont plus directement ou intégralement stockées ou traitées par ses capacités « internes » mais sont envoyées dans le cloud afin de bénéficier des avantages en termes d'espace de stockage et de puissance de calcul offerts par ce service. En outre, l'utilisation du *cloud* par le robot lui permet de bénéficier des données traitées ou créées par d'autres robots.

12. Risques – Les risques pour la vie privée et familiale et pour la sécurité des données que présentent un robot victime d'une cyberattaque sont légions. On pense dans un premier temps aux dommages physiques et matériels qui peuvent être causés par un robot de service contrôlé par un tiers malintentionné. Il en va ainsi du robot qui place un objet dangereux à portée d'un enfant, qui lance ou dépose les clefs du domicile à l'extérieur de celui-ci, ou encore du robot qui s'en prend directement aux personnes. On pense dans un second temps à la collecte non-consentie de données et à la diffusion de celles-ci. Il en est ainsi du robot dont les données sont interceptées par un tiers ou du robot qui, directement contrôlé par un tiers, capte des conversations ou des images censément privées[32].

Une fois encore, le risque de prise de contrôle d'un objet connecté ne constitue pas une nouveauté ou un phénomène exclusif aux robots. On pense, entre autres, aux questionnements quant à la sécurité des webcams et des caméras de surveillance connectées installées à l'intérieur du domicile. Cependant, l'ampleur de l'atteinte à la vie privée rendue possible par la corruption d'un robot est renforcée par le fait que celui-ci est capable de se mouvoir et d'interagir physiquement avec son environnement. Disposant de telles capacités, le robot est capable d'enregistrer une plus grande variété de données et fait peser une menace plus grande sur la vie privée et la sécurité du domicile[33].

SECTION 6. – L'aspect social des robots

13. Robotique émotionnelle – Une autre dimension de la robotique est également de nature à venir rendre plus ténue la protection de la vie privée des utilisateurs. Cette dimension est liée à la relation que l'être humain peut tisser avec un robot, *a fortiori* si celui-ci tend à ressembler

[32] *Ibid.*, p. 6.

[33] R. CALO, « Robots and Privacy », *op. cit.*, p. 193.

à l'être humain. Il ne paraît pas inopportun de parler de réel « aspect social » de la robotique[34] ou encore, de robotique émotionnelle[35].

La robotique émotionnelle peut être définie comme l'ensemble des techniques utilisées par les roboticiens pour créer chez l'homme une empathie envers le robot. Des exemples simples permettent de comprendre comment les roboticiens peuvent s'y prendre pour créer ce lien émotionnel : le robot ressemble à un être humain (on parle alors de robot anthropoïde), le robot fait usage d'attitudes humaines (il se penche pour parler à un utilisateur triste, il pose sa main sur l'épaule d'une personne en colère...), son visage recrée des mimiques humaines, il emploie un vocabulaire adapté à la personne avec laquelle il communique...[36]. La robotique émotionnelle n'est pas, en tant que telle, une technique utilisée avec une intention malicieuse. Au contraire, elle est utilisée pour faciliter les interactions entre l'homme et le robot. En effet, un robot qui adopte des comportements « humains » sera plus facilement accepté par ses utilisateurs et sera, par conséquent, plus apte à remplir les fonctions pour lesquelles il a été programmé[37].

14. Transfert émotionnel – L'utilisation de la robotique émotionnelle présente toutefois un danger. Celui-ci réside dans le transfert émotionnel qui s'effectue en faveur du robot. Ainsi, un utilisateur peut être amené – parce que son robot a une forme et adopte des attitudes qui ressemblent à celle de l'homme ou encore d'un animal familier – à éprouver pour la machine les sentiments qu'il éprouverait pour un autre humain ou pour un animal[38]. Il s'agit là d'une forme d'anthropomorphisme.

[34] *Ibid.*, p. 195.

[35] N. Nevejans, *Étude pour la Commission JURI sur les règles européennes de droit civil en robotique*, Commission des affaires juridiques du Parlement européen, 2016, PE 571.379, p. 27.

[36] R. Gelin et O. Guilhem, *Le robot est-il l'avenir de l'homme ?*, Paris, La Documentation française, 2016, pp. 9-10.

[37] K. Darling, « Extending legal protection to social robots: The effect of anthropomorphism, empathy and violent behavior towards robotic objects », *Robot Law* (R. Calo, A. M. Froomkin et I. Kerr dir.), Cheltenham, Edward Elgar, 2016, p. 218 ; N. Nevejans, *Étude pour la Commission JURI sur les règles européennes de droit civil en robotique*, *op. cit.*, p. 27.

[38] Kate Darling donne plusieurs exemples de transferts émotionnels en faveur du robot. Ainsi, les possesseurs du robot-chien Aibo déclarent éprouver des remords lorsqu'ils remettent le robot dans sa boite. Dans le même sens, les participants à une étude sur l'empathie envers les robots refusent de détruire le robot-dinosaure Pleo après avoir interagi avec lui, certains participants allant même jusqu'à physiquement empêcher que le robot soit frappé. L'exemple le plus connu est sans doute celui de l'interruption des tests opérationnels d'un robot-démineur par l'armée américaine. Le robot, qui avait approximativement la forme d'un phasme, perdait l'un de ses membres après chaque explosion de mine. Après cinq explosions, le colonel qui supervisait l'exercice demanda l'arrêt des tests car il ne pouvait supporter la vue du robot peinant à se déplacer sur le membre dont il disposait encore (K. Darling, « Extending legal protection to social robots: The effect of anthropomorphism, empathy and violent behavior towards robotic objects », *op. cit.*, pp. 216-225 et les références citées).

Éprouvant pour le robot des sentiments identiques à ceux éprouvés envers une véritable personne, l'utilisateur risque de ne plus considérer celui-ci comme une machine capable de collecter des données sur sa vie privée. Considérés comme des personnes et non plus comme des moyens de collecte de données, les utilisateurs se montrent alors moins vigilants envers les robots qu'ils ne le sont envers un formulaire administratif ou une étude de marché et sont plus enclins à révéler des informations intimes[39].

15. Risques – En outre, le robot se révèle être un bien meilleur collecteur d'informations que ne l'est un humain. Nous l'avons vu, le robot peut faire usage de comportements humains qui vont créer de l'empathie chez l'utilisateur. Cependant, alors même qu'il peut faire usage de comportements propres à l'Homme, le robot ne présente pas les « défauts » inhérents à la personne humaine. Ainsi, il jouit d'une mémoire parfaite, n'est potentiellement jamais atteint par la « fatigue » ou la « lassitude »[40], et dispose de senseurs capables d'analyser nos réactions bien plus finement qu'un œil humain. La conjonction de ces facteurs fait du robot un outil de collecte de données théoriquement très performant[41].

Ces capacités dans la collecte de données peuvent susciter une certaine forme d'inquiétude. Ainsi, il n'est pas impossible que l'aspect social du robot et sa « ressemblance » avec l'Homme soient expressément utilisés pour faciliter la collecte de données ou à des fins de marketing ciblé par les compagnies qui mettent les robots sur le marché[42].

[39] *Ibid.*, p. 221.

[40] R. Calo, « Robots and Privacy », *op. cit.*, pp. 196-197.

[41] D. M. Cooper, « The application of a "sufficiently and selectively open license" to limit liability and ethical concerns associated with open robotics », *Robot Law* (R. Calo, A. M. Froomkin et I. Kerr dir.), Cheltenham, Edward Elgar, 2016, pp. 177-178.

[42] R. Calo, « Robots and Privacy », *op. cit.*, p. 197 ; R. Gelin et O. Guilhem, *Le robot est-il l'avenir de l'homme ?*, *op. cit.*, p. 10 ; K. Darling, « Extending legal protection to social robots: The effect of anthropomorphism, empathy and violent behavior towards robotic objects », *op. cit.*, p. 221 ; C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *op. cit.*, p. 3.

SECTION 7. – Un manque de connaissance des utilisateurs

16. *Black box* – Le droit à la vie privée des utilisateurs de robots peut également – de manière plus transversale – être mis à mal par le manque de connaissances ou d'informations concernant le fonctionnement des robots et la manière dont les données des utilisateurs sont collectées, stockées et traitées.

Cette absence de connaissance dans le chef des utilisateurs est connue sous le nom de « *black box problem* ». Appliquée au robot, la métaphore de la boite noire peut être décrite de la manière suivante : l'utilisateur donne une information au robot (*input*), le robot traite cette information au moyen d'algorithmes dont le fonctionnement échappe à l'utilisateur (*black box*), le robot adopte un comportement – observable par l'utilisateur – sur base de l'information qu'il a traitée (*output*).

L'analphabétisme technologique dans lequel se trouvent les utilisateurs vis-à-vis de la robotique est prévisible. La compréhension des algorithmes et de la programmation informatique en général restent aujourd'hui des compétences pointues accessibles uniquement à un public spécialement formé[43].

Cette absence de connaissances relatives au fonctionnement du robot a pour conséquence de placer l'utilisateur dans une situation de vulnérabilité. Son ignorance quant à la manière dont les données sont collectées et traitées l'empêche de contrôler la pertinence de ces opérations et augmente le risque d'utilisation abusive de ces informations[44].

CHAPITRE 2. Le GDPR, source de solutions ou de blocages ? Une question de point de vue

17. Pertinence de l'étude – Après avoir mis en exergue de quelles manières les robots pouvaient porter atteinte à la vie privée des individus qui seront amenés à être en contact, plus ou moins volontairement, avec ceux-ci, nous allons tâcher d'étudier le cadre juridique applicable aux traitements de

[43] J. Burrell, « How the machine "thinks" : Understanding opacity in machine learning algorithms », *Big Data Society*, 2016, p. 4.

[44] C. Castets-Renard, « Traitement algorithmique des activités humaines : le sempiternel face à face homme / machine », *Cahiers Droit, Sciences & Technologie*, 6/2016, p. 242 ; C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *op. cit.*, p. 3.

données privées, ou données à caractère personnel[45] pour utiliser l'expression consacrée. Le robot traite en effet constamment des données à caractère personnel, que ce soit celles de son propriétaire ou de tiers.

18. L'adoption du GDPR – Cette matière a récemment subit une profonde refonte puisqu'en 2016, le Parlement européen et Conseil de l'Union européenne adoptèrent un nouveau Règlement (le Règlement général sur la protection des données, ci-après « GDPR ») venant remplacer l'ancienne directive[46] qui datait d'il y a plus de vingt ans.

Ce nouveau texte ne révolutionne pas fondamentalement la matière de la protection des données mais l'adapte aux réalités actuelles en introduisant une série de nouveautés censées d'une part, renforcer les droits des citoyens dont les données sont traitées (ci-après « personnes concernées ») et, d'autre part, faciliter la vie des responsables de ces traitements[47] en supprimant certaines démarches administratives.

19. Une étude complexe – Ce texte récent – qui ne sera d'ailleurs applicable qu'à partir du 25 mai 2018[48] – fait actuellement l'objet de questionnements sur bon nombre de points. Il demeure donc une certaine incertitude sur l'interprétation à donner à plusieurs dispositions de ce nouveau Règlement. Dès lors, l'étude de l'application du GDPR au monde des robots est un exercice périlleux tant qu'aucun document du Comité européen de la protection des données – remplaçant le Groupe de travail de l'article 29 (ci-après G29) – ne précise comment il faut interpréter certains passages du GDPR et comment appliquer les concepts du GDPR aux robots.

20. Structure du chapitre – Malgré ces incertitudes, nous tenterons d'analyser en quoi le GDPR permettrait d'empêcher la survenance des différents risques soulevés précédemment[49] et en quoi celui-ci pourrait

[45] Donnée à caractère personnel : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale », définition donnée à l'article 4, 1), du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE, *J.O.U.E.*, L 119, 4 mai 2016.

[46] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L 281, 23 novembre 1995.

[47] Pour les objectifs du Règlement voy. considérants 4 et s. du GDPR.

[48] Art. 99 du GDPR.

[49] Voy. Chapitre 1.

également représenter un frein au développement des robots dans la mesure où le GDPR fixe un cadre juridique relativement strict pour le traitement de données à caractère personnel (Section 2). Pour ce faire, nous tenterons, avant tout de chose, d'identifier correctement, au sens du GDPR, les différentes personnes qui pourraient être considérées comme responsable des traitements effectués par un robot (Section 1).

21. Champ d'étude – Précisons que nous concentrons notre propos sur les robots utilisés sous la responsabilité de particuliers ou d'entreprises et non pas d'organismes publics. Le GDPR prévoit pour ces responsables de traitement d'un genre un peu particulier une série de spécificités et d'exceptions que nous n'aborderons pas dans le cadre de cette contribution.

SECTION 1. – Qui est responsable des traitements de données à caractère personnel opérés par un robot ?

22. Une étape préalable nécessaire – Avant d'étudier les nombreuses règles imposées aux responsables de traitement et les droits des personnes concernées, il est nécessaire d'identifier qui est le responsable du traitement quand un robot traite une donnée à caractère personnel.

Cette étape préalable est primordiale puisqu'elle permet, premièrement, de savoir si le traitement entre ou non dans le champ d'application matériel du GDPR et ensuite, à qui incombe le respect des différentes obligations prévues dans le GDPR[50].

Nous commencerons donc par brièvement rappeler le champ d'application du GDPR et comment identifier correctement un responsable de traitement et un sous-traitant.

§ 1. Champ d'application du GDPR

23. Principe – Tout traitement de données personnelles réalisé sur le territoire européen doit en principe respecter le GDPR[51]. Cependant, l'article 2,

[50] Voy. Chapitre 2, Section 2.

[51] Pour plus de détails voy. art. 2 et 3 du GDPR. L'article 3 prévoit également que le GDPR s'applique « en cas de traitement de données personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées soit a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union ».

paragraphe 2, du GDPR prévoit notamment que le règlement ne s'applique pas au traitement de données à caractère personnel effectué : « [...]

c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique [...] ».

Par traitement de données à caractère personnel, il faut comprendre « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »[52]. Sans rentrer dans les détails de cette notion, il est évident qu'un robot traite des données à caractère personnel, ou pour être plus exact même, le robot est un moyen technique (comme un ordinateur) permettant à quelqu'un (son utilisateur, ou le fabricant du robot) de traiter des données personnelles dans un but spécifique[53].

24. Étendue de l'exception pour usage personnel ou domestique – Le point c) de l'article 3 précise donc que le GDPR ne s'applique pas au traitement effectué par une personne physique dans le cadre d'une activité strictement personnelle ou domestique. À l'occasion de l'affaire *Frantisek* tranchée par la CJUE et que nous évoquerons plus en détails dans les lignes qui suivent, l'avocat général précisait que, selon lui, les activités personnelles sont « les activités étroitement et objectivement liées à la vie privée d'une personne qui ne touchent pas de manière sensible à la sphère personnelle d'autrui » et les activités domestiques sont les activités « liées à la vie familiale [qui] ont normalement lieu au sein du domicile »[54].

Si l'exception est libellée dans des termes quasiment identiques à ceux de de la directive[55], le considérant 18 du GDPR[56] pourrait modifier l'étendue de cette exception et rendre éventuellement caduque une partie de la jurisprudence de la Cour de Justice relative à cette question.

[52] Art. 4, 2), du GDPR.

[53] Pour savoir qui, juridiquement, traite les données voy. *infra*, § 3.

[54] Concl. av. gén. N. JÄÄSKINEN, pt 51 à l'occasion de l'arrêt C.J.U.E., 11 décembre 2014, *Frantisek*, C-212/13.

[55] Art. 3, § 2, second tiret, de la directive 95/46 : « effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques ».

[56] À savoir « [l]e présent règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Les activités personnelles ou domestiques pourraient inclure l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités

Le considérant 18 inclut explicitement dans cette exception « l'utilisation de réseaux sociaux et les activités en ligne » à titre non professionnel ou commercial, alors que la Cour avait – dans un arrêt *Lindqvist*[57] – estimé que « cette exception doit être interprétée comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des particuliers, ce qui n'est pas manifestement pas le cas du traitement de données à caractère personnel consistant dans leur publication sur Internet de sorte que ces données sont rendues accessibles à un nombre indéfini de personnes »[58]. Une autre manière de voir les choses serait d'envisager que ce considérant 18 ne modifie pas en réalité la portée de l'exception et qu'il faut donc toujours appliquer la jurisprudence de la Cour et faire la distinction entre *les publications rendant accessibles certaines données à un nombre indéfini de personnes* et les autres.

Le GDPR ne semble *a priori* pas remettre en cause le second arrêt de la Cour[59] en la matière. La Cour était en l'espèce amenée à trancher la question de savoir si l'utilisation d'une caméra filmant une partie de la rue pouvait encore être considérée comme une « activité qui s'insère [exclusivement] dans le cadre de la vie privée ou familiale des particuliers »[60]. La Cour avait alors répondu, que « dans la mesure où une vidéosurveillance telle que celle en cause au principal s'étend, même partiellement, à l'espace public et, de ce fait, est dirigée vers l'extérieur de la sphère privée de celui qui procède au traitement des données par ce moyen, elle ne saurait être considérée comme une activité exclusivement personnelle ou domestique »[61]. Cet arrêt, et particulièrement les conclusions de l'avocat général, demeurent éclairants mais cette jurisprudence est-elle encore d'actualité dans la mesure où le considérant 18 nous semble élargir la portée de cette

en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ».

[57] C.J.C.E., 6 novembre 2003, *Lindqvist*, C-101/01. Pour un commentaire de l'arrêt voy. C. DE TERWANGNE, « Arrêt Lindqvist ou quand la Cour de Justice des Communautés européennes prend position en matière de protection des données personnelles », note sous C.J.C.E., 6 novembre 2003, *R.D.T.I.*, 2004, n° 19, pp. 67 à 99.

[58] C.J.C.E., *Lindqvist*, précité, § 47. La Cour rappela sa position dans l'arrêt CJUE, 16 décembre 2008, *Satamedia*, C-73/07.

[59] C.J.U.E., *Frantisek*, précité.

[60] Notion utilisée par la Cour dans son arrêt *Lindqvist* (§ 47) pour apprécier la portée de l'exception domestique. Le terme « exclusivement » a été rajouté par nos soins puisque dans son arrêt *Frantisek* (§ 31) la Cour reprend cette formulation et rajoute ce terme, en rappelant que celui-ci était présent dans le libellé de la directive 95/46. Pour une étude plus détaillée voy. C. DE TERWANGNE, « L'exception concernant les traitements de données à des fins personnelles et domestiques de la directive 95/46 relative à la protection des données », note d'observations sous C.J.U.E., 11 décembre 2014, *R.D.T.I.*, 2015, pp. 39-51.

[61] C.J.U.E., *Frantisek*, § 33, précité.

exception[62] ? Il ne nous semble cependant pas que l'enseignement de cet arrêt soit remis en question par l'entrée en vigueur du GDPR mais rien n'est certain et nous nous interrogeons encore sur la manière d'interpréter précisément ce considérant 18. Vient-il profondément modifier la notion d'exception pour usage personnel ou domestique, ou ne fait-il qu'effacer ce qu'avait décidé la Cour dans son arrêt *Lindqvist* ?

Concernant cette exception, il reste deux autres points à régler, points particulièrement importants pour le cas de traitements effectués par des robots. Le premier concerne la question de savoir comment régler la situation où, en cas de responsabilité conjointe entre plusieurs responsables de traitement, un responsable bénéficie de cette exception et l'autre pas. Le second porte sur la manière d'interpréter le final de ce fameux considérant 18 précisant que « toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques ». Une manière de l'interpréter serait de dire qu'en cas de responsabilité conjointe où un des responsables bénéficie de l'exception pour usage personnel ou domestique, l'autre responsable reste tenu de respecter le GDPR, ce qui répond alors partiellement la première question. Cependant, la référence au sous-traitant n'est dans ce cas pas pertinente, sauf à considérer que le sous-traitant d'un responsable de traitement bénéficiant de l'exception pour usage personnel ou domestique – n'étant donc pas soumis aux règles imposées par le GDPR, doit lui respecter les obligations qui incombent aux sous-traitants en vertu du GDPR, ce qui nous parait aberrant.

Nous reviendrons sur ces questions une fois que nous étudierons les cas spécifiques aux robots.

§ 2. Notion de « responsable de traitement » et « sous-traitant »

25. Définition – Le Règlement définit le responsable de traitement comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [...[63]] »[64].

[62] Dans le même sens voy. B. VAN ALSENOY, « I tweet therefore I am... subject to data protection law », dispo. sur www.law.kuleuven.be/citip/blog.

[63] « [...], lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

[64] Art. 4, 7), du GDPR.

26. Seul ou Conjointement – La définition prévoit explicitement que cette responsabilité peut être partagée et ainsi reposer sur plusieurs personnes différentes. Précisons que le GDPR consacre son article 26 à régler les questions soulevées par cette situation.

27. « Détermine les finalités et les moyens du traitements » – Concrètement, déterminer les finalités d'un traitement signifie désigner les objectifs de celui-ci, et déterminer les moyens[65] signifie la manière d'y parvenir : le « pourquoi » et « le comment »[66].

Dans le cas où plusieurs personnes distinctes s'entendent pour effectuer un traitement, celui qui décide dans quel but les données sont traitées doit être qualifié systématiquement de responsable de traitement. Celui qui ne détermine que les « moyens » ne pourra par contre être considéré comme responsable de ce traitement que si ce dernier a plus de marge de manœuvre que n'aurait un simple sous-traitant. Tel sera le cas lorsqu'il décide « d'aspects essentiels qui sont traditionnellement et intrinsèquement réservés à l'appréciation du responsable du traitement, tels que "quelles sont les données à traiter ?", "pendant combien de temps doivent-elles être traitées ?", "qui doit y avoir accès", etc. »[67].

28. Sous-traitant – À l'inverse, une personne – même si elle n'a reçu que des instructions vagues – ne disposant que d'une marge de manœuvre sur des éléments peu importants[68] sera considérée comme un sous-traitant, à savoir « une personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement »[69].

29. Appréciation factuelle – L'appréciation de ces différents rôles s'effectue sur base des circonstances de fait. Pour cela, il y a lieu de voir, dans chaque cas, qui a l'autorité pour déterminer les caractéristiques principales d'un traitement : son objectif, ses méthodes...

Les éléments contenus dans un contrat entre plusieurs parties (attribution des tâches de chacun...) doivent être pris en compte pour apprécier sur qui repose la responsabilité du traitement mais ces éléments doivent cependant refléter la situation réelle. La désignation dans un contrat

[65] Cela comprend aussi bien les moyens techniques (quel logiciel) qu'organisationnel (qui peut avoir accès aux données, où elles sont stockées...) voy. G29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, WP 169, 16 février 2010.

[66] *Ibid.*, p. 14.

[67] *Ibid.*

[68] *Ibid.*

[69] Art. 4, 8), du GDPR.

d'une partie comme responsable de traitement ne suffit donc pas pour qualifier celle-ci de responsable du traitement au sens du droit relatif à la protection des données. Et à l'inverse, se faire désigner comme sous-traitant ne permet pas d'échapper aux différentes obligations attribuées au responsable de traitement.

30. Une réalité complexe – La définition de responsable de traitement et de sous-traitant paraissent relativement claires, mais les traitements de données sont devenus d'une complexité (nombreuses données, nombreux acteurs) qui rend difficile l'indentification du ou des responsable(s) de traitement, et le cas des traitements effectués au moyen de robots en est un parfait exemple.

§ 3. Les différentes situations possibles concernant la responsabilité des traitements effectués au moyen d'un robot

31. Des pistes de réflexion – Dans la mesure où la qualification des différentes parties prenant part à un traitement de données personnelles doit se faire sur une base factuelle[70], il existe une multitude de configurations possibles. Nous allons donc dégager certains critères spécifiques aux robots qui permettront d'effectuer, dans chaque cas, cette identification des responsables de traitement(s).

Nos propos sont avant tout là pour tracer des pistes de réflexion sur la façon de réfléchir à la qualification des différents acteurs en présence et non pour affirmer que telle personne doit être considérée comme responsable. Cela restera toujours en définitive une appréciation au cas par cas.

32. Le terme « utilisateur » – Avant toute chose, précisons que nous recourrons au sein de cette section au terme *utilisateur* pour qualifier la personne qui a un pouvoir de contrôle effectif sur le robot. Si cette personne n'est pas un particulier mais un employé agissant au nom et pour compte d'une entreprise, le terme *utilisateur* fera alors référence à l'entreprise, et non la personne physique qui a autorité sur le robot. De fait, les employés d'une entreprise agissant pour celle-ci ne sont, en principe, pas considérés comme responsables de traitement, seule l'entreprise peut l'être[71]. De plus, si plusieurs utilisateurs ont autorité sur le robot, les deux parents dans une famille par exemple, ceux-ci seront alors responsables conjoints des traitements effectués par leur robot. Nous ne rentrerons pas plus dans les questions qui pourraient survenir si un enfant demande

[70] Voy. *supra*, n° 29.

[71] Pour plus de précision sur ce point voy. G29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, *op. cit.*, pp. 15 et s.

quelque chose à un robot ou le cas de désaccord entre plusieurs personnes qui auraient autorité sur un robot et donc en partie sur les traitements que celui-ci effectue. Cette question s'appréciera de manière casuistique.

A. En fonction des lieux et des usages

33. Au sein du domicile – Pour rendre les choses concrètes, prenons l'exemple d'un robot (téléguidé par son propriétaire, répondant aux consignes données par celui-ci ou respectant un schéma d'actions choisi par celui-ci) qui filme et enregistre ce que les gens font et disent à l'intérieur de la maison de son propriétaire, pour s'assurer que tout va bien chez lui, pour surveiller ses enfants ou garder des souvenirs (films, photos...) des moments importants de sa vie.

Dans ce cas-ci, l'utilisateur du robot va pouvoir bénéficier, sans difficulté, de l'exception pour usage strictement personnel ou domestique vu que ce traitement est effectué *exclusivement dans sa sphère personnelle ou domestique*[72].

34. À la limite du domicile – Imaginons maintenant que ce robot surveille également dans le jardin et, à l'occasion de ses déplacements – en tournant par exemple –, filme parfois également la rue[73], sans toutefois que cela soit volontaire de la part du robot ou de son utilisateur. Dans ce cas, est-on encore, dans le champ d'application de cette exception personnelle ou domestique ? Sauf à suivre aveuglément la réponse de la Cour dans l'arrêt *Frantisek*[74], à nos yeux, si l'extérieur du domicile n'est filmé que de manière très accessoire et involontairement, on resterait dans le champ de l'exception. Même si les exceptions doivent toujours être interprétées strictement[75], il nous semble qu'elle continue de s'appliquer dans la mesure où cette situation « ne touche pas de manière sensible à la sphère personnelle d'autrui »[76].

35. À l'extérieur du domicile – Cependant, si ce robot ne se contente plus de filmer à l'intérieur du domicile de son propriétaire, et filme dans la rue[77], comme les drones, alors l'utilisateur de ce robot ne bénéficiera plus de cette exception vu que ce type de traitement n'est plus effectué exclusivement au sein d'un domicile et porte *sensiblement atteinte à la sphère personnelle d'autrui* (des passants...).

[72] Voy. *supra*, n° 24.

[73] Cela peut aussi être le cas lorsqu'un robot mobile filme à l'intérieur d'une maison présentant des fenêtres donnant sur la rue.

[74] Voy. *supra*, n° 24.

[75] C.J.U.E., *Frantisek*, § 29.

[76] Concl. av. gén. N. JÄÄSKINEN, § 51 à l'occasion de l'arrêt C.J.U.E., *Frantisek*, précité.

[77] Étant entendu que nous partons du principe qu'il effectue un traitement de données à caractère personnel.

Ainsi, toute personne utilisant un robot qui traite des données à caractère personnel en dehors de son domicile, se devra de respecter le GDPR. Nous ne voyons en effet que peu d'hypothèses où un traitement effectué par un robot, hors du domicile du responsable de ce traitement, pourrait être une *activité personnelle* qui ne porterait pas *sensiblement atteinte à la sphère personnelle d'autrui*. Les pouvoirs de récolte d'informations sont tels que, quasi-systématiquement, il y aura une atteinte à la vie privée des autres personnes.

B. En fonction de la complexité du robot

36. Les robots simples – Reprenons l'exemple du robot qui filme et enregistre ce que les gens font et disent, sans que ces données ne soient analysées ou transmises ailleurs. Cette situation est simple dans la mesure où seul l'utilisateur du robot décide quelles données sont traitées, pourquoi elles le sont... Il est même le seul à traiter ces données. L'utilisateur détermine donc seul les finalités et les moyens du traitement, ce qui fait de lui l'unique responsable de ce traitement.

37. Les robots sophistiqués – Dans le premier exemple nous prenions le cas de l'utilisateur du robot étant le seul à *déterminer les finalités et les moyens du traitement de données*.

Qu'en est-il quand plusieurs acteurs rentrent en ligne de compte ?

Cela arrive pour ainsi dire tout le temps avec des robots dotés d'une intelligence artificielle plus développée, capables de récolter via leurs différents capteurs des données, de les analyser et de réagir en conséquence, sans que cette réaction soit toujours prévisible par l'utilisateur du robot[78]. L'utilisateur ne sait pas forcement à chaque fois ce que va faire le robot, ni pourquoi il le fait et encore moins comment.

En effet, afin de fonctionner et effectuer des tâches un peu complexes, ces robots « intelligents » doivent être connectés à internet pour accéder à certaines ressources externes hébergées dans le cloud (informations stockées ailleurs, capacité supplémentaire de calcul ou de stockage...) et tout cela souvent sans même que l'utilisateur du robot ne s'en rende compte.

Dès lors, comment peut-on encore considérer que, dans ces hypothèses où l'utilisateur ne comprend pas ce qui se passe concrètement, l'utilisateur du robot soit considéré comme seul responsable des différents traitements effectués par son robot dont il n'a même pas conscience ? De fait, il ne sait ni ne décide exactement et précisément quelles données sont récoltées

[78] « *Black box problem* » voy. *supra*, n° 16.

par son robot, l'utilisation qui en est faite concrètement (transfert, classement, analyse...). La seule chose qu'il contrôle plus ou moins, ce sont les demandes qu'il fait au robot. Et même dans ce cas, il n'est véritablement conscient que de ce qu'il a demandé et pas toujours de ce que sa demande va nécessiter comme traitement de données personnelles d'autrui. Nous n'irons toutefois pas jusqu'à dire que l'utilisateur du robot ne doit pas être considéré comme responsable de traitement. En effet, en pouvant généralement paramétrer largement ce que peut et doit faire son robot, il détermine, la plupart du temps, en partie suffisante, les modalités principales du fonctionnement de son robot et des traitements de données nécessaires à son fonctionnement pour être considéré comme responsable de traitement.

L'entreprise, qui a conçu et mis sur le marché ce robot, qui gère toutes les ressources extérieures au robot – mais indispensables à son fonctionnement –, est-elle encore un simple sous-traitant de l'utilisateur du robot ou responsable conjoint des traitements avec ce dernier ? La différence est parfois difficile à faire mais, selon nous, bien souvent cette entreprise est la seule qui détermine concrètement quel type de données sera récolté par le robot, comment elles seront analysées, comment et où les données seront transférées. Ces choix dépassent, dans certains cas, largement la marge de manœuvre d'un simple sous-traitant et ressemble plus aux prérogatives d'un responsable de traitement.

Nous n'avons n'envisagé ici que le cas de robots conçus de A à Z par une seule entreprise et ne fonctionnant que grâce à des ressources sous le contrôle de cette seule entreprise, ce qui est relativement rare actuellement. Il est donc fort probable que plusieurs sociétés soient en réalité, en fonction des cas, sous-traitants de cette entreprise ou même responsables conjoints avec celle-ci et l'utilisateur du robot.

38. Résumé – En conséquence, nous pensons que dans de nombreux cas, les traitements effectués au moyen de robots relèvent, selon nous, aussi bien de la responsabilité de l'utilisateur du robot que de l'entreprise qui gère concrètement les processus internes et externes du robot.

C. En fonction des finalités

39. Pour l'utilisateur ou le fabricant ? – Les robots sont des machines traitant une série impressionnante de données pour une série de raisons différentes. Nous n'avons parlé pour le moment que de traitements de données, sans préciser les différentes raisons pour lesquelles celles-ci étaient traitées.

Il faut pourtant faire la distinction entre les données qui sont traitées pour permettre au robot d'offrir certaines fonctionnalités et les données

récoltées par ce robot à destination uniquement du fabricant du robot[79]. D'un côté, les données sont traitées au profit de l'utilisateur du robot et de l'autre les données sont traitées au profit de l'entreprise (finalité propre à l'entreprise) et non de l'utilisateur.

« Dans certains cas, différents acteurs traitent les mêmes données à caractère personnel les uns à la suite des autres. Dans ce cas, il est probable qu'au niveau individuel, les différentes opérations de traitement de la chaîne semblent déconnectées, chacune d'elles pouvant avoir une finalité différente. Il sera néanmoins nécessaire de vérifier si, d'un point de vue global, les opérations de traitement ne doivent pas être considérées comme un "ensemble d'opérations" poursuivant une finalité commune ou utilisant des moyens déterminés conjointement »[80].

Pour la première catégorie de traitements, la responsabilité des traitements peut reposer sur l'utilisateur du robot et/ou de son fabricant en fonction des cas[81] puisqu'ils utilisent d'un point de vue global, des moyens déterminés conjointement[82]. Pour la seconde, la responsabilité repose uniquement sur l'entreprise. Ainsi, certaines finalités seront considérées comme commune à tous les responsables et d'autres non.

Cette distinction est également importante pour savoir, pour chaque traitement, si l'utilisateur du robot est une personne concernée (qui a des droits) ou un responsable de ce traitement. Il est donc possible d'être tantôt responsable des traitements effectués par son robot et tantôt personne concernée pour les traitements de données réalisés par ce robot.

§ 4. Comment assurer une protection efficace des données personnelles dans ces différentes situations ?

40. Les cas de responsabilité conjointe – Ces situations sont relativement rassurantes puisqu'elles permettent de faire peser la responsabilité du respect du GDPR sur au moins un professionnel qui aura normalement les ressources et les connaissances nécessaires pour assurer la conformité des différents traitements dont il est responsable selon le GDPR, ce que n'a pas forcément un particulier lambda. De plus, il est plus facile pour le fabricant du robot d'effectuer, à chaque nouveau modèle de robot produit, le travail

[79] Ces données peuvent par exemple être revendue ensuite par l'entreprise à des tiers ou être utilisées afin d'enrichir des bases de données du fabricant pour parfaire et améliorer le fonctionnement de ces robots...

[80] G29, *Avis 1/2010 sur les notions de « responsable du traitement » et de « sous-traitant »*, *op. cit.*, p. 29.

[81] Voy. *supra*, A et B.

[82] Sur la question de la responsabilité conjointe voy. *supra*, n° 27.

nécessaire pour s'assurer que les traitements de données effectués par ce nouveau modèle respectent le GDPR. Ce travail consisterait notamment à intégrer ces considérations relatives au GDPR dès la conception du robot (*privacy by design*)[83] et à monter un dossier GDPR[84]. Il suffirait ensuite au fabricant d'expliquer – éventuellement sous la forme de formation, ou en proposant un service de DPO-as-a-service[85] – à chaque acheteur du robot comment utiliser les facultés du robot tout en respectant le GDPR.

Comme pour tout cas de responsabilité conjointe, les responsables conjoints doivent se répartir – de manière transparente et respectueuse du rôle réel de chacun – les obligations respectives[86]. Il est prévu que le droit communautaire ou d'un État membre puisse également déterminer les responsabilités de chacun[87]. Il serait judicieux d'user de cette possibilité afin d'éviter que certaines sociétés fassent finalement reposer injustement l'ensemble des obligations sur la partie plus faible qu'est le futur acquéreur du robot ayant face à lui un contrat-type rédigé à l'avance par la société.

Demeure toutefois la question de savoir comment régler les situations où un des responsables conjoints bénéficie de l'exception pour usage personnel ou domestique, comme cela sera généralement le cas pour les robots-compagnons. Selon nous, le considérant 18 du GDPR[88] précise que, dans ce cas, les autres responsables doivent respecter le GDPR. Dès lors, concrètement, ils doivent pour ainsi dire assurer seuls le respect du GDPR, en contrôlant eux-mêmes ce que pourra faire l'utilisateur du robot comme traitement de données avec celui-ci. Cela pourrait notamment passer par des mesures techniques de blocage incorporées dans le robot (forme avancée de *privacy by design*[89]) ou des interdictions rappelées dans une notice d'utilisation, par exemple.

41. L'utilisateur comme unique responsable de traitement – Dans les cas où l'utilisateur du robot, simple particulier, est seul responsable du traitement de données, ne bénéficiant pas de l'exception pour usage personnel ou domestique, il semble illusoire de croire que le GDPR sera

[83] Voy. chapitre 2, Section 2, § 3.

[84] Ce dossier reprendrait en détails toutes les spécificités des traitements de données personnelles effectués par le robot et préciserait en quoi ceux-ci sont conformes au GDPR.

[85] Service consistant à assurer les fonctions normalement attribuées à un DPO. Le DPO (*data protection officer*) est chargé de veiller, au sein d'une entreprise généralement, au respect du GDPR. Pour plus de détails sur la fonction, voy. G29, *Guidelines on data protection officers*, WP 243, 13 december 2016.

[86] Art. 25 du GDPR.

[87] *Ibid.*

[88] Voy. *supra*, n° 24.

[89] Voy. chapitre 2, Section 2, § 3.

respecter par celui-ci. Le GDPR risque alors de vite connaitre le même sort que la directive 95/46 : devenir un texte inconnu et peu respecté. Les particuliers qui vont utiliser des robots ne sont de fait, contrairement aux entreprises (et encore), pas conscients du cadre règlementaire applicable aux traitements de données à caractère personnel, et ne sont même parfois pas conscients qu'ils effectuent pareils traitements.

42. Des solutions au manque de connaissances des utilisateurs-responsables de traitement – Pour éviter cela, plusieurs solutions sont envisageables. La première consiste à considérer qu'un consommateur désireux d'acquérir un robot doit être informé par le vendeur que le robot effectuera plus que probablement des traitements de données à caractère personnel, et que dès lors, il faudra respecter le cadre légal existant, à savoir le GDPR. Le traitement de données personnelles nous semble en effet être une caractéristique principale du robot[90] et donc une information à communiquer obligatoirement avant toute vente d'un robot à un consommateur. Cela ne permettra pas de faire respecter en tant que tel le GDPR mais au moins à faire prendre conscience de son existence, charge au consommateur d'ensuite faire le nécessaire pour se conformer à cette législation.

Ceci nous laisse, avouons-le, relativement perplexe. C'est pourquoi à nos yeux, il faut tant que possible que, lors de la conception des robots, les différents éléments du GDPR soient au maximum intégrés dans le code même du robot, de sorte qu'un utilisateur lambda qui « malgré lui » est responsable de traitement n'ait pas trop à faire pour que les traitements effectués par son robot respectent dans une large mesure les prescrits du GDPR. Ce principe est imposé au responsable de traitement, mais dans notre hypothèse, le fabricant du robot n'est justement pas responsable du traitement, il n'a donc pas formellement l'obligation de respecter le principe de *privacy by design*[91].

Pour obliger les fabricants à intégrer ce principe, une solution pourrait être d'imposer à certains types de robots amenés à traiter des données à caractère personnel une certification « GDPR compliant » et donc *privacy by design*, que leur fabricant soit responsable conjoint des traitements ou non, que l'utilisateur du robot bénéficie ou pas de l'exception pour usage personnel ou domestique. Le GDPR ne permet pas d'imposer cela, mais pourquoi ne pas alors imposer pour certains types de robot,

[90] Art. 5, § 1, a), de la directive 2011/83/UE du Parlement européen et du Conseil du 25 octobre 2011 relative aux droits des consommateurs, modifiant la directive 93/13/CEE du Conseil et la directive 1999/44/CE du Parlement européen et du Conseil et abrogeant la directive 85/577/CEE du Conseil et la directive 97/7/CE du Parlement européen et du Conseil, *J.O.U.E*, L 304, 22 novembre 2011.

[91] Voy. *infra*, n° 57.

particulièrement susceptible de mettre à mal la vie privée de chacun, une autorisation préalable de mise en circulation sur le marché dont l'une des conditions serait cette certification ?

SECTION 2. – Les réponses, pas toujours adaptées, du GDPR

43. Préambule – Dans cette section, nous tenterons de voir comment le GDPR pourrait éviter les atteintes à la vie privée évoquées précédemment[92]. Si le GDPR apporte éventuellement certaines solutions, celles-ci sont parfois difficiles à mettre en place dans le monde des robots, où de nombreux traitements de données personnelles s'effectuent constamment, et où la machine au moyen de laquelle sont effectués ces traitements est capable de se mouvoir et prendre des décisions sans que le responsable de celle-ci soit forcément conscient de cela.

Vu qu'il nous était impossible de passer en revue l'ensemble des dispositions du GDPR dans le cadre de cette contribution (des ouvrages entiers étant consacrés à ce sujet), nous avons sélectionné une série de points du GDPR qui permettraient d'empêcher que les robots ne mettent, en toute légalité, en danger notre vie privée.

§ 1. Licéité du traitement

44. Principe de licéité du traitement – Un robot effectue un grand nombre de traitements de données personnelles et tout traitement de données à caractère personnel doit être licite.

Pour être licite, un traitement doit répondre à au moins une de ces conditions :

a) « la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;

[92] Voy. *supra*, chapitre 1.

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant »[93].

En ce qui concerne les robots, plusieurs sources de licéité sont envisageables (le consentement, l'intérêt légitime ou la nécessité pour un contrat)[94]. Celles-ci varieront en fonction du type de traitement, des circonstances...

45. Données sensibles – Pour les données considérées comme sensibles[95], le traitement de celles-ci n'est possible que dans un nombre limité de cas[96], l'un des plus fréquents étant le consentement explicite de la personne concernée.

Ce type de données étant soumis à un régime spécifique, les robots devraient être capables techniquement d'identifier automatiquement ce type particulier de données pour les traiter de manière particulière, voire ne pas les traiter du tout s'il n'a pas de raison spécifique de le faire. Cette capacité d'identification est particulièrement nécessaire dans les cas où, par exemple, lors d'une conversation avec son utilisateur, le robot serait amené par celui-ci à traiter certaines données révélant ses orientations politiques, données que le robot devrait éventuellement analyser pour adapter son discours. Dans ce cas, le robot traitera des données sensibles et devra donc avoir notamment recueilli un consentement explicite de la personne pour le traitement de ce type de données. Une autre solution serait de solliciter systématiquement ce consentement spécifique pour prévoir ce genre de situations où l'utilisateur demande au robot – sans forcément s'en rendre compte – de traiter des données sensibles le concernant.

46. Un consentement valable de la personne concernée – Quand le traitement est fondé sur le consentement de la personne concernée, ce consentement doit être libre, spécifique à une finalité précise, éclairé et

[93] Art. 6, § 1, du GDPR.

[94] D'autres sont envisageables dans des situations particulières. Pour les robots capables de sauver des vies comme certaines robots compagnons, nous pourrions invoquer comme base de licéité la sauvegarde d'un intérêt vital (art. 6, point d), du GDPR).

[95] À savoir les données révélant « l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique », art. 9 du GDPR.

[96] Voy. art. 9 du GDPR.

univoque[97]. Ce consentement peut être exprimé par écrit ou par un acte positif claire (forme de consentement tacite)[98].

47. Comment initier légalement le contact robot-humain ? Pour rentrer en contact avec quelqu'un et réagir de manière la plus humaine possible[99], un robot a besoin d'effectuer des traitements de données personnelles. Il a par exemple besoin de filmer la personne ou d'enregistrer ces propos pour vérifier s'il connait déjà cette personne, d'analyser son ton de voix pour adapter ses propos à l'humeur de la personne[100]... et tout ça avant même d'avoir commencé à véritablement discuter avec cette personne. Simplement pour vérifier que la personne a éventuellement déjà donné son consentement pour traiter des données la concernant, le robot va être amené à traiter des données personnelles (acquisition d'une photo de la personne, reconnaissance faciale, confrontation avec la liste des personnes enregistrées, vérification d'un éventuel consentement)[101].

Cette problématique n'est pas neuve et existe depuis l'apparition des systèmes biométriques et de reconnaissance faciale. Dès lors, pour les opérations de traitements préalables à la demande et à l'obtention du consentement, il a été considéré acceptable de fonder le traitement sur l'intérêt légitime du responsable du traitement[102]. Passer par l'intérêt légitime nécessite de prendre des mesures afin de limiter l'atteinte aux droits de la personne concernée. Pour ce faire, il suffit simplement que le robot efface les informations qu'il a utilisées après ce laps de temps si finalement la personne ne consent pas aux traitements effectués par le robot[103].

48. Pour les utilisateurs « réguliers » – Pour les utilisateurs réguliers du robot, le plus simple consiste à passer par un consentement éclairé de ces personnes. Ainsi pour les robots domestiques[104], il suffirait la première

[97] Voy. définition du consentement donnée à l'article 4, 11) du GDPR. Pour plus de détails, voy. art. 8 et consid. 32 du GDPR ; G29, *Avis 15/2011 concernant la définition du consentement*, WP 187, 13 juillet 2011.

[98] *Ibid.*

[99] Sur cette tendance au mimétisme et les risques que cela peut engendrer au regard de la vie privée voy. chapitre 1, section 6.

[100] Certaines de ces opérations peuvent ne pas constituer des traitements de données à caractère personnel si le robot ne procède pas à une identification de la personne mais analyse par exemple simplement le ton de sa voix, de manière totalement anonyme. Cette minimisation des traitements de données personnelles est en principe obligatoire, voy. *infra*, § 2.

[101] G29, *Avis 02/2012 sur la reconnaissance faciale dans le cadre des services en ligne et mobiles*, W192, 22 mars 2012, p. 6.

[102] *Ibid.*

[103] *Ibid.*

[104] Rappelons que, dans ce genre de cas de figure, le propriétaire du robot ne doit pas respecter le GDPR (exception pour usage personnel ou domestique, voy. *supra*, n^{os} 33 et s.) mais le fabricant pourrait très bien lui le devoir (voy. *supra*, n° 39).

fois que le robot « entre en contact » avec une personne présente dans la maison qu'il lui explique quelles données il va collecter et pourquoi il le fait[105] et demande ensuite le consentement de la personne. Cette solution reste relativement facile à mettre en place et peu contraignante.

Une autre possibilité consiste à dire que les traitements de données effectués par ce robot sont nécessaires pour le faire fonctionner et donc nécessaires à l'exécution du contrat conclu entre le fabricant du robot et le propriétaire de celui-ci. Cette solution permet d'éviter de demander explicitement le consentement mais il reste difficile de déterminer qui est partie au contrat : seul l'acheteur ou les membres de sa famille restreinte également ?

49. Les personnes qui sont volontairement rentrées en contact avec le robot – Pour ces personnes, il est envisageable de considérer qu'elles ont consenti de manière tacite (en posant un acte positif pour reprendre les termes du GDPR[106]) à certains traitements, à savoir ceux notamment nécessaires pour que le robot puisse tenir une conversation avec la personne (reconnaissance faciale, analyse du langage, éventuellement création d'un profil, mémorisation de la discussion en cas de nouvelle rencontre,...) ou faire ce que cette personne lui demande. En effet, ces personnes ont fait volontairement la démarche de venir se présenter au robot pour interagir avec ce dernier et sont en principe conscientes de ce que, pour fonctionner, le robot a besoin de traiter certaines données personnelles les concernant. Peut se poser la question de savoir si la personne a véritablement consenti de manière éclairée puisque, le robot, dans un souci de convivialité, n'a pas forcément donné l'ensemble des informations nécessaires[107] pour que la personne puisse valablement donner son consentement. Toutefois, dans quelques années, il est probable que la plupart des individus soient davantage conscients de ce qui se passe techniquement quand on discute avec un robot.

En principe, le robot devra effacer l'ensemble de ces données si aucune raison ne justifie qu'il les conserve plus longtemps (principe de minimisation des données)[108].

50. Les tiers involontaires – Si pour les personnes « fréquentant » régulièrement un robot, il est préférable de prendre le temps, une fois pour toutes, d'obtenir un consentement de la personne, cette option n'est

[105] Une série d'autres informations doit être donnée avant d'obtenir un consentement éclairé. Voy. *infra*, n° 59.

[106] Voy. *supra*, n° 44.

[107] Voy. art. 7 et consid. 42 du GDPR.

[108] Voy. *infra*, § 2.

pas envisageable quand le robot circule en rue et traite des données sur une série de personnes qu'il a croisées, avec qui il a discuté... On envisage mal demander le consentement de chaque passant. Ce genre de robots va cependant probablement créer des profils pour chaque personne avec qui il a interagi pour permettre d'assurer éventuellement une continuité dans la relation avec ces personnes... Si on souhaite qu'un robot ressemble le plus possible à un humain, il faut que celui-ci ait au moins cette capacité de mémoire relationnelle avec des tiers occasionnels.

Pour les personnes qui ne font pas cette démarche active vers le robot, le consentement tacite n'est pas possible. Il faudra dès lors que le robot demande le consentement de ces personnes s'il souhaite traiter des données les concernant.

Il est également possible de passer dans certains cas par l'intérêt légitime du responsable de traitement, si cela n'est pas disproportionné par rapport aux atteintes portées aux droits de la personne concernée. Par exemple, pour pouvoir interagir avec les personnes qu'il connait, le robot a besoin au préalable d'effectuer une reconnaissance faciale de toutes les personnes qu'il croise pour ensuite identifier celle qu'il connait. Il va donc traiter des données biométriques d'une multitude de gens. Il peut le faire légitimement s'il efface au fur et à mesure les données non pertinentes[109].

51. Privacy by design – Rappelons que bien souvent, le robot qui circule en rue, ne traitera pas forcément de données personnelles des passants s'il est suffisamment *privacy by design*[110].

§ 2. Limitation des traitements de données (principe de finalité et de minimisation)

52. Une tendance à la collecte de toutes données utiles – Un robot, s'il n'est pas *privacy by design*[111], aura tendance à récolter un maximum de données, en enregistrant souvent plus de données que nécessaire, au cas où... D'une certaine manière, du point de vue d'un fabricant de robot, cela peut se comprendre puisqu'en récoltant ces données, le fabricant peut d'une part essayer d'améliorer le fonctionnement du robot et d'autre part essayer de tirer un maximum d'informations pour tenter d'en déduire lui-même certaines choses ou tout simplement les revendre à une

[109] Même idée que celle développée précédemment au point 47.

[110] Précisons qu'un robot n'est pas censé traiter plus de données personnelles que celles nécessaires. Voy. *infra*, § 2 et § 3 et note de bas de page 100.

[111] Voy. *infra*, § 3.

autre entreprise intéressée[112]. Tout le contraire des principes contenus dans le GDPR.

53. Deux principes clés – Pour éviter justement qu'on ne traite des données personnelles sans raison et de manière disproportionnée, ce qui porterait atteinte à la vie privée de chacun, il existe deux grands principes en protection des données à caractère personnel : le principe de finalité et le principe de minimisation.

54. Principe de finalité – Toute donnée personnelle doit être traitée dans un but précis, limité, et déterminé à l'avance et, en principe, uniquement dans ce but-là[113]. Si le traitement n'est pas fondé sur le consentement de la personne, il n'est possible de réutiliser ces données que si elles ne sont pas traitées ultérieurement de manière incompatible[114] avec les finalités initiales justifiant la collecte des données. Pour apprécier cette compatibilité, il faudra notamment tenir compte : de l'existence éventuelle d'un lien entre les finalités pour lesquelles les données à caractère personnel ont été collectées et les finalités du traitement ultérieur envisagé, du contexte, de la nature, des conséquences possibles du traitement ultérieur envisagé pour les personnes concernées et de l'existence de garanties appropriées[115]. Si le traitement est fondé sur le consentement de la personne concernée, la réutilisation est impossible si cela n'a pas été indiqué à la personne au moment de l'obtention de son consentement. Il faudra donc redemander un consentement pour cette nouvelle réutilisation des données.

Précisons que dans tous les cas, il est interdit de revendre à un tiers des données personnelles sans en informer clairement la personne concernée[116].

Rappelons que la réutilisation de données anonymisées peut être effectué librement, celles-ci ne sont en effet, par définition, plus des données personnelles puisqu'elles ne peuvent être rattachées à une personne identifiée[117], le GDPR ne s'applique donc plus.

Pour des traitements très précis et ciblés, identifier à l'avance les finalités s'avère assez facile. Tel est par exemple le cas d'un numéro de téléphone qui est généralement récolté uniquement pour pouvoir contacter la personne.

[112] Voy. par exemple la polémique à propos d'un robot aspirateur qui enregistrerait le plan des maisons pour ensuite les revendre à d'autres entreprises : http://www.lesnumeriques.com/aspirateur-robot/doit-on-craindre-qu-irobot-revende-cartographies-roomba-n65181.html

[113] Art. 5, b), du GDPR.

[114] Art. 6, § 4, du GDPR.

[115] *Ibid.*.

[116] Art. 13, § 3, du GDPR.

[117] Voy. définition de données à caractère personnel, art. 4, 1), du GDPR.

Quand il est question de données personnelles récoltées au moyen de robots de plus en plus polyvalents, il devient difficile de définir précisément, à l'avance, pour quelles raisons telle donnée est récoltée si ce n'est pour assurer le bon fonctionnement du robot et des très nombreuses actions qu'il peut réaliser.

Les robots étant amenés à devenir de véritables couteaux-suisses qui pourront effectuer des tâches très variées en fonction de l'environnement dans lequel ils vivront, déterminer précisément à l'avance la liste probablement très longue des différentes finalités, pour chaque donnée récoltée, risque de poser certaines difficultés pratiques quand on voit le niveau de détails exigé pour l'identification des finalités des traitements. « Assurer le bon fonctionnement du robot » n'est en effet pas suffisant. Tous les traitements de donnés opérés par le robot se coupent et recoupent, ils interagissent les uns avec les autres, de manière très dynamique. Lister alors toutes les finalités des traitements que peut effectuer un robot reste envisageable – même si fastidieux – au moment de sa mise en marche. Cela s'avère toutefois quasi impossible de tenir cette liste à jour, surtout si les fonctionnalités (donc traitements) de ce robot évoluent en fonction du temps, comme c'est le cas pour les robots auto-apprentisants qui pourraient eux-mêmes créer de nouvelles fonctionnalités, de leur propre initiative ou lorsque quelqu'un leur a enseignées (sans que cette personne ne se rende forcément compte qu'elle lui apprend et lui demande d'effectuer un nouveau traitement de données personnelles). Tous ces nouveaux traitements ne sont, en principe, possibles que s'ils sont compatibles avec la(les) finalité(s) initiale(s). Une certaine partie le seront probablement mais pas tous, il faudra alors demander un consentement aux personnes concernées pour ces nouvelles fonctions (traitements), ce qui reste difficile, voire impossible, à réaliser en pratique.

55. Principe de minimisation des données – Le second principe prévoit qu'on ne peut traiter des données personnelles que si celles-ci sont nécessaires à l'accomplissement de la finalité pour lesquelles elles ont été collectées (principe de minimisation)[118]. Ce principe vaut aussi bien pour la durée de conservation que le volume de données. Comme indiqué précédemment, il est déjà difficile d'identifier clairement les différentes finalités mais alors déterminer quelle donnée est (encore) nécessaire pour atteindre la(les) finalité(s) pour la(les)quelle(es) a été récoltée, et pas simplement potentiellement utile pour un éventuel futur nouveau traitement, peut vite devenir ardu. Un système d'effacement des données inutilisées pendant un certain temps nous parait donc un moyen simple de

[118] Art. 5, c), et consid. 39 du GDPR.

répondre, *a minima*, à cette obligation de minimisation des données. Si l'effacement n'est pas toujours faisable, il reste alors possible de procéder à une anonymisation des données. Ainsi pour reprendre l'exemple d'un passant en rue qui a discuté avec un robot et que cela ait automatiquement provoqué la création d'un profil dans sa base de données (pour assurer une continuité dans les discussions avec la personne...), ce profil peut être effacé après quelques semaines (comme un humain oublierait cette discussion), alors que pour une personne croisée tous les jours par le robot (un voisin), ce délai avant effacement pourrait être de plusieurs mois ou années. Cela permettrait de transposer d'une certaine manière le fonctionnement de la mémoire humaine au robot en classant les différents types de personnes rencontrées et en adaptant la durée de conservation en fonction.

§ 3. Privacy by design

56. Le principe – Le GDPR impose maintenant à tout responsable de traitement de prendre en compte le droit de la protection des données au moment de la conception, et non à la fin de ce processus, et ainsi mettre en place des mesures techniques et organisationnelles appropriées pour garantir le respect des exigences du règlement[119]. « Ces mesures pourraient consister, entre autres, à réduire à un minimum le traitement des données à caractère personnel, à pseudonymiser les données à caractère personnel dès que possible, à garantir la transparence en ce qui concerne les fonctions et le traitement des données à caractère personnel, à permettre à la personne concernée de contrôler le traitement des données, à permettre au responsable du traitement de mettre en place des dispositifs de sécurité ou de les améliorer »[120]. Appliqué au robot, cela signifie par exemple que les robots circulant en rue floutent automatiquement les visages des passants, les plaques de voiture... qu'il n'a pas, ou plus, besoin d'identifier[121]. Cela évite ainsi de traiter des données personnelles inutilement (minimisation des données)[122].

[119] Art. 25 du GDPR.

[120] Considérant 78 du GDPR. Sur le sujet voy. les travaux de Ann Cavoukian, *Information and Privacy Commissioner*, Ontario, Canada qui est à l'origine de ce concept, particulièrement « Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices », December 2012, dispo. sur http://www.ontla.on.ca/library/repository/mon/26012/320221.pdf ; B. PRENEEL and D. IKONOMOU (dir.), *Privacy Technologies and Policy : First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*, Berlin, Springer, 2014.

[121] Concernant les drones, voy. Futur of privacy forum, « Drones and Privacy by Design : Embedding Privacy Enhancing Technology in Unmanned Aircraft », August 2016, dispo. sur https://fpf.org/wp-content/uploads/2016/08/Drones_and_Privacy_by_Design_FPF_Intel_PrecisionHawk.pdf

[122] Voy. *supra*, § 2.

Ce principe est capital pour assurer une efficacité maximale des règles contenues dans le GDPR. Les véritables choix sont en effet posés bien souvent par les concepteurs de logiciels, d'applications, de robots et pas forcément par ceux qui les utilisent pour traiter des données personnelles de tiers. La manière dont les données sont traitées a été fixée en majeure partie par le concepteur et non par le responsable de traitement ignorant bien souvent les détails techniques du logiciel, de l'application... qu'il utilise. De plus, si le concepteur respect ce principe, il réduit les possibilités de traitements de données contraires aux prescrits du GDPR et limite donc techniquement les possibles abus.

57. Une obligation pour le concepteur ? Même si dans la plupart des travaux concernant la robotéthique[123] et l'éthique dans le développement de l'intelligence artificielle, tout le monde s'accorde à dire que les concepteurs doivent respecter ce principe de *privacy by design*, il n'en demeure pas moins que juridiquement, le respect du principe de *privacy by design* repose sur le responsable de traitement et non sur les concepteurs, qui eux ne traitent pas de données personnelles. Ainsi, le fabricant d'un drone n'est pas tenu de respecter l'article 25 du GDPR imposant le *privacy by design*, seul l'utilisateur de ce drone – en tant que responsable des traitements effectués par le drone[124] – devra prouver qu'il a choisi un drone qui permet de respecter le GDPR, c'est-à-dire un drone « *privacy by design* ». Rien n'empêche donc actuellement la vente de robots qui effectueront des traitements de données ne respectant pas le GDPR.

Dès lors, comment s'assurer qu'un particulier intéressé par l'achat d'un drone choisisse un drone « *privacy by design* » qui sera probablement plus cher que ceux n'intégrant pas ces technologies de protection de la vie privée ? Soit en conscientisant l'acheteur soit en contrôlant la mise sur le marché des robots.

Face à des consommateurs, le vendeur a un devoir d'information sur les caractéristiques principales du robot[125] et donc du fait que ce robot effectuera, plus que probablement, des traitements de données personnelles, traitements dont l'acheteur devra assurer la conformité avec le GDPR.

[123] Voy. par exemple le rapport d'IEEE, E*thically aligned design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems*, dispo. sur http://standards.ieee.org/develop/indconn/ec/ead_v1.pdf ; Rapport de Mady Delvaux pour le Parlement européen contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)), A8-0005/2017, 27 janvier 2017.

[124] Sur la question de la responsabilité conjointe éventuelle entre le fabricant du robot et son utilisateur, et les conséquences juridiques de ce partage, voy. *supra*, Chapitre 2, Section 1 (point 40).

[125] Voy. *supra*, n° 42.

Sinon, il serait possible de conditionner la mise sur le marché de robots traitant des données personnelles à une certification « GDPR compliant »[126]. Cela permettrait de s'assurer que tous les robots présents en Europe sont « *privacy by design* ».

§ 4. Droits des personnes concernées

Le GDPR accorde une série de droits aux personnes concernées. Ces droits permettent à la personne concernée de pouvoir d'une part être informée de l'utilisation qui est faite des données la concernant, et d'autre part avoir un certain contrôle sur celles-ci.

58. Modalité d'exercices des droits de la personne concernée – Avant d'évoquer ces différents droits[127], attardons-nous sur les modalités d'exercice de ceux-ci. Le responsable doit – dans la mesure du possible – faciliter l'exercice des droits de la personne concernée et répondre aux demandes de celle-ci dans les meilleurs délais[128].

Si pour un utilisateur quotidien du robot, l'exercice ne pose pas véritablement de problème et est facile à mettre en place vu la relation étroite qu'il a avec ce robot et donc souvent avec le(s) responsable(s) de celui-ci. Pour les tiers qui, à un moment, ont été, ou pensent être l'objet d'un traitement de données de la part de ce robot qui circulait en rue, il peut s'avérer compliqué de pouvoir contacter le responsable de ce traitement. Deux solutions sont possibles selon nous : soit le robot peut lui-même être capable de répondre directement aux demandes de ces personnes, soit il est indiqué physiquement sur le robot le nom du responsable[129] et ses coordonnées, comme l'impose l'article 13, a), du GDPR. Cependant, pour éviter également de trop porter atteinte à la vie privée du propriétaire du robot[130], il nous parait préférable d'opter pour un système de numéro d'immatriculation, comme pour les voitures. Certes, cette solution pourrait être – dans une certaine mesure – contraire à l'article 13 mais elle permet de concilier la vie privée du propriétaire du robot et les droits accordés aux personnes concernées par un traitement de données. Cette solution semble relativement facile à mettre en place mais il faudra alors créer un service chargé de faire l'intermédiaire entre le responsable de traitement et la personne concernée. L'identité du responsable de traitement

[126] Sur les certifications voy. *infra*, n° 72.

[127] Pour plus de détails sur ces droits nous renvoyons aux articles 12 à 22 du GDPR.

[128] Pour plus de précision voy. art. 12, § 2, et considérant 58 du GDPR.

[129] Le robot pourrait également indiquer, sur demande, qui contacter.

[130] On pourrait en effet apprendre beaucoup de choses sur la vie privée de ceux-ci en pouvant facilement savoir à qui appartient tel robot et en sachant ce que ce robot fait.

ne serait alors révélée que dans certains cas bien spécifiques. Ce service pourrait parfaitement être géré par les fabricants de robots, ce qui permettrait ainsi à ces derniers de répondre directement eux-mêmes aux demandes, d'autant plus qu'ils sont selon nous, dans de nombreux cas, responsables conjoints des traitements et qu'ils pourraient donc être désignés[131] comme personne à contacter si une personne concernée souhaite exercer l'un de ses droits. De plus, les fabricants sont mieux à même de répondre efficacement aux différentes demandes que les simples particuliers ayant acheté un de leurs robots. Ils connaissent de fait mieux la législation relative à la protection des données, peuvent mobiliser plus de moyens pour un suivi efficace des demandes et ont probablement déjà la possibilité d'accéder aux données stockées par le robot.

59. Droit d'information – Toute personne a le droit de savoir si des données la concernant sont traitées et dans ce cas d'obtenir une série d'informations[132] :

« a) les finalités du traitement ;

b) les catégories de données à caractère personnel concernées ;

c) les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées ;

d) lorsque cela est possible, la durée de conservation des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée

[...]

g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute information disponible quant à leur source ;

h) l'existence d'une prise de décision automatisée, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée ».

Cette dernière information revêt une importance particulière quand la décision est prise par un robot et non un être humain[133]. En effet, la personne concernée peut avoir du mal à comprendre pourquoi un robot réagit de telle manière face à elle. Ces informations concernant la logique

[131] Comme cela peut être prévu en vertu de l'article 26 du GDPR.

[132] Pour une liste complète voy. art. 15 du GDPR.

[133] Rappelons que les robots prennent des décisions en fonction d'algorithmes conçus à l'origine par des humains. Pour une étude plus détaillée des questions liées à l'éventuelle généralisation des décisions automatisées voy. la contribution d'Antoinette Rouvroy intitulée « La robotisation de la vie ou la tentation de l'inséparation ».

sous-jacente du traitement permettent ainsi de lutter contre ce qu'on appelle le « *black box problem* »[134].

En plus de ces informations, le responsable du traitement doit communiquer à la personne concernée, au moment de la collecte des données, certaines informations le concernant et l'informer du fait, qu'en tant que personne concernée, elle a une série de droits[135].

60. Droit d'opposition – La personne concernée a le droit de s'opposer, « pour des raisons tenant à sa situation particulière »[136], au traitement de ses données si le traitement se base sur l'intérêt légitime du responsable de traitement. Concernant les robots, ce droit revêt une importance particulière vu que le consentement des personnes est relativement difficile à obtenir et que les traitements sont donc bien souvent effectués sur base de l'intérêt légitime du responsable de traitement. Si une personne concernée fait usage de ce droit, le responsable du traitement sera alors contraint d'effacer les données la concernant, « à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée »[137].

61. Droit à l'effacement – Le responsable de traitement devra également supprimer les données se rapportant à quelqu'un si cette personne ne consent plus à ce que celles-ci soient conservées dans la mémoire du robot[138], si la finalité pour laquelle elles ont été récoltées a été remplie[139] ou encore si ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles sont traitées[140][141].

62. Droit à ne pas faire l'objet d'une décision automatisée – La personne a également « le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire »[142]. Cette disposition est fondée sur l'idée que la dignité de l'homme impose le droit de ne pas être complètement soumis à la décision d'une machine.

[134] Voy. *supra*, n° 16.

[135] Voy. art. 13, 14 et 15 du GDPR.

[136] Art. 21, § 1, du GDPR.

[137] *Ibid.*

[138] Art. 17, b), du GDPR.

[139] Principe de minimisation des données, voy. *supra*, n° 55.

[140] *Ibid.*

[141] D'autres motifs peuvent justifier cette demande d'effacement, voy. art. 17 du GDPR.

[142] Art. 22 du GDPR. Un rejet automatique d'une demande de crédit en ligne ou des pratiques de recrutement en ligne sans aucune intervention humaine constitue des traitements affectant de manière significative la personne concernée, voy. consid. 71 du GDPR.

Les robots, par définition, seront amenés à prendre *des décisions fondées exclusivement sur un traitement automatisé, y compris le profilage produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire*[143]. Une forme de consentement de la personne est cependant nécessaire pour effectuer pareil traitement. Comment alors les robots peuvent-ils fonctionner en cas de refus de consentement ? À l'heure actuelle, aucune exception prévue à ce droit[144] ne permettrait juridiquement à un robot de prendre, par lui-même, certaines décisions affectant significativement des humains, sans une forme de consentement de la part de ces personnes. Aucun intérêt légitime du responsable de traitement ne peut venir palier cette absence de consentement. Dès lors, dans le cas de traitements opérés par les robots, où ceux-ci prennent constamment des décisions de manière automatique, ce droit ne viendrait-il pas d'une certaine manière limiter la portée de l'article 6, paragraphe f) qui permet de fonder un traitement sur l'intérêt légitime du responsable de traitement ? Ce droit permettrait donc, dans une certaine mesure, à la personne concernée de s'opposer à ce qu'un robot prenne certaines décisions l'affectant significativement et donc concrètement, de bloquer certaines capacités du robot nécessitant la prise d'une décision automatique basée sur un traitement des données de cette personne.

63. Droit de rectification – La personne concernée peut exiger que les données inexactes qui la concernent soient corrigées[145].

64. Droit à la portabilité des données – Enfin, le GDPR introduit un nouveau droit particulièrement intéressant quand il s'agira de changer de robot et de passer à un autre modèle de la marque ou à un modèle venant d'un concurrent : le droit à la portabilité des données[146].

[143] Pour prendre un exemple assez caricatural mais aisément compréhensible, imaginons un robot-vigile qui refuse l'accès à un magasin à certaines personnes au motif que – sur base de leur apparence physique – ces personnes sont catégorisées par le robot comme « personnes à risque ». Prendre pour exemple un robot-vigile n'est pas anodin. De fait, à l'heure actuelle, les législations réglementant certaines professions sont pensées pour des humains. Or, certaines de celles-ci risquent d'être exercées à l'avenir par des robots, ce qui pourrait nécessiter de revoir ces législations. Ainsi, il n'y aurait aucun sens d'imposer, comme c'est le cas pour les agents de sécurité par exemple, certaines conditions quant à leurs casiers judiciaires...

[144] Les exceptions listées à l'article 22, 2 c), du GDPR sont la nécessité pour la conclusion ou l'exécution d'un contrat entre la personne concernée et un responsable du traitement, l'autorisation par le droit de l'Union ou d'un État membre, ou le consentement *explicite* de la personne concernée.

[145] Art. 16 du GDPR.

[146] Art. 20 du GDPR.

Sans rentrer dans les détails de cette disposition aux contours encore imprécis[147], ce droit permettra par exemple à la personne concernée de solliciter de son fournisseur l'extraction d'une partie de ses données personnelles stockées dans la mémoire d'un robot pour les mettre dans celle d'un autre.

§ 5. Sécurité

65. Réalité actuelle – Les robots ont vocation à prendre une place toujours plus grande dans nos vies et vont progressivement traiter des données parfois très intimes et personnelles[148]. Si tout le monde s'accorde à dire que la sécurité est quelque chose de vital[149], il n'en demeure pas moins qu'actuellement les robots mis sur le marché ne traitent pas ces données de manière parfaitement sécurisée et utilisent parfois des canaux de communication peu protégés[150], ce qui permet à des personnes mal intentionnées d'intercepter ces données.

66. Une obligation pourtant – Le GDPR impose pourtant que toutes les données personnelles « soient traitées de façon à garantir une sécurité appropriée [de celles-ci], y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées »[151].

Le responsable de traitement doit donc adopter un niveau de sécurité adapté « compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques »[152].

Cette sécurité passera notamment par « la pseudonymisation et le chiffrement des données à caractère personnel ; des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ; des moyens

[147] Pour une étude détaillée de l'article 20 voy. G29, *Guidelines on the right to « data portability »*, WP 242, 13 décembre 2016.

[148] Données de santé, données relatives à des enfants...

[149] Voy. *supra*, chapitre 1, section 5.

[150] Récemment certains jouets connectés ont d'ailleurs fait l'objet de nombreuses critiques et notamment sur le manqué de sécurité de ceux-ci, voy. https://www.quechoisir.org/action-ufc-que-choisir-jouets-connectes-alerte-sur-la-securite-et-les-donnees-personnelles-n23355/ ; sur le sujet de la sécurité des robots domestiques voy., T. Dennings, C. Matuszk, K. Koscher, J. R. Smith et T. Kohno, « A Spotlight on Security and Privacy Risks with Future Household Robots : Attacks and Lessons », *op. cit.*

[151] Art. 5, f), du GDPR.

[152] Art. 32 du GDPR.

permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ; une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement »[153].

67. Analyse d'impact – Pour apprécier ce niveau de risque, le GDPR impose, dans certains cas[154], la réalisation d'une *analyse d'impact relative à la protection des données* qui a pour but d'identifier les risques potentiels et ainsi pouvoir mettre en place des mesures de protection adéquates pour éviter la survenance de ceux-ci.

En ce qui concerne les robots, il faudra obligatoirement passer par cette étape puisqu'elle est obligatoire en cas « d'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire »[155], ce que font constamment les robots[156].

68. Un produit sûr – Encore une fois, cette obligation de sécurité repose sur le responsable de traitement et pas forcément sur le fabricant du robot. Cependant, à nos yeux, un robot ne peut être considéré comme *sûr*, s'il ne garantit pas un niveau de sécurité suffisant pour empêcher quiconque de pouvoir intercepter les données personnelles qu'il traite ou de prendre le contrôle du robot[157]. Il ne devrait, dès lors, pas pouvoir être mis sur le marché en vertu notamment de la directive Machines[158].

§ 6. Flux transfrontières

69. Une multitude de flux – La plupart du temps, pour fonctionner les robots ont besoin d'être connectés à un réseau, et ainsi accéder à certaines ressources hébergées dans le *cloud*. Ceux-ci ne disposent notamment pas d'assez de puissance pour traiter localement toutes les données. Ces données (personnelles bien souvent) sont donc envoyées sur des serveurs pour

153 *Ibid.*
154 Voy. art. 35 du GDPR.
155 Art. 35, § 3, a), du GDPR.
156 Voy. *supra*, n° 62.
157 Voy. *supra*, n^{os} 11 et 12 et références citées.
158 Sur l'application de la directive Machines au robot, voy. N. Nevejans, *Traité de droit et d'éthique de la robotique civile*, Bordeaux, LEH édition, 2017, pp. 284-304.

être analysées de manière plus efficace, ce qui peut constituer un flux transfrontière si ces serveurs ne sont pas localisés en Europe.

70. Limites légales – Ces flux transfrontières de données personnelles ne sont, en principe, autorisés que vers des pays tiers ayant un niveau de protection adéquat[159]. Dans la mesure où actuellement la Commission européenne n'a reconnu comme *pays assurant un niveau de protection adéquat* que quelques pays[160] dont les principaux sont la Suisse, l'Argentine, le Canada[161], et les États-Unis[162], les données personnelles ne pourront pas quitter l'espace européen, sauf si le responsable de traitement prévoit « des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives »[163]. Ces garanties peuvent consister, notamment[164], en des clauses contractuelles entre les différentes parties aux transferts, des règles d'entreprises contraignantes, un engagement contraignant à suivre un code de conduite, ou une certification[165].

Il est également possible d'effectuer le transfert si la personne concernée, informée des risques d'un pareil transfert, a explicitement consenti à celui-ci[166].

Il est donc loin d'être impossible d'effectuer des flux transfrontières mais, encore une fois, cette localisation des serveurs est prévue par le fabricant du robot qui n'est pas forcément le responsable des traitements de données, ce qui pose problème[167].

159 Art. 45 du GDPR.
160 Les pays – où des sociétés spécialisées dans la fabrication de robots sont implantées – seraient d'ailleurs bien inspirés de tenter de se faire reconnaitre comme *pays assurant un niveau de protection adéquat*, pour faciliter ces transferts de données.
161 Pour les transferts à destination de sociétés devant respecter la loi canadienne du 13 avril 2000 sur la protection des renseignements personnels et les documents électroniques.
162 Pour les transferts à destination de sociétés respectant les principes du « *Privacy Shield* ». Rappelons cependant que ce « *Privacy shield* » est l'objet de très nombreuses critiques. Il n'apporterait, selon ses détracteurs, toujours pas suffisamment de garanties et risquerait donc de connaitre le même sort que son prédécesseur, le « Safe Harbor », annulé par la C.J.U.E. Sur ce sujet voy. M. Bernaerts, « Les transferts de données à caractère personnel entre l'Union européenne et les États-Unis : une valse à mille temps ? », *R.D.C.-T.B.H.*, 2017/2, pp. 161-184.
163 Art. 46, § 1, du GDPR.
164 Pour une liste complète et détaillée voy. art. 46, §§ 2 et s., du GDPR
165 Sur ces deux derniers points, voy. *infra*, § 7.
166 Art. 49 du GDPR. Cet article prévoit d'autres dérogations à l'interdiction de transfert dans certaines situations particulières.
167 Voy. *supra*, n^{os} 40 à 42.

§ 7. Code de conduite et certification

71. Code de conduite – Compte tenu de la spécificité des différents secteurs auxquels le GDPR s'appliquera, il est prévu que les représentants de catégories particulières de responsables de traitement peuvent élaborer des codes de conduite qui auront vocation à préciser les modalités d'application du GDPR sur à ce secteur d'activité. Ces codes seront alors soumis à approbation d'une autorité de contrôle nationale ou du Comité européen de protection des données, si des activités de traitement sont menées dans plusieurs États membres[168]. Un contrôle doit alors être prévu pour vérifier que chaque responsable de traitement respecte ce à quoi il s'est engagé.

Il est fort à parier que pareils codes de conduite verront le jour pour les traitements effectués par les robots. Cela aura le mérite de clarifier les choses et fixer un cadre spécifique aux robots.

72. Certification – Un responsable de traitement a également la possibilité d'obtenir une certification de conformité de ses traitements accordée par des organismes habilités à délivrer ce type de certification[169].

Ces mécanismes permettraient aux fabricants et exploitants de robots de démontrer que leurs robots sont conformes aux prescrits du GDPR mais pas forcément que le GDPR est respecté puisqu'il n'est pas possible *a priori* de contrôler l'usage qui en sera fait par chaque utilisateur de ce modèle de robot. Cependant, nous pourrions envisager de conditionner la mise sur le marché de ces robots à l'obtention d'une certification ou l'engagement à suivre un code de conduite.

Conclusion

73. Cadre juridique dépassé – Nous l'avons vu, les réglementations protectrices de la vie privée et des données à caractère personnel actuellement en vigueur semblent parfois peu adaptées à l'émergence des robots dans nos quotidiens.

Ce constat n'est pas neuf. La régulation légale des nouvelles technologies est une discipline complexe. Deux raisons peuvent expliquer les difficultés que présentent l'adoption d'une législation pertinente et efficiente dans ce domaine.

[168] Art. 40 du GDPR.

[169] Voy. art. 42 et 43 du GDPR.

74. Loi et technologie – Premièrement, la loi et les technologies ont une perception du temps diamétralement opposée. Là où l'acte législatif inscrit – ou devrait inscrire – son adoption dans le temps long nécessaire à la réflexion, les technologies apparaissent, évoluent et changent constamment. La loi paraît donc condamnée à être dépassée par l'avènement des technologies. De ce fait, l'action législative dans ce domaine semble devoir se confiner à une approche réactive. Une technologie surgit, le législateur évalue les conséquences de celle-ci sur l'environnement juridique, une loi est éventuellement adoptée pour encadrer la technologie nouvelle.

Cette chronologie n'est toutefois pas une fatalité. Ainsi, une norme adoptée à un temps donné et présentant un degré d'indétermination relativement élevé peut présenter la flexibilité nécessaire pour être appliquée à des situations qui n'était peu ou pas prévisibles au moment de son adoption[170]. Toutefois, l'adoption d'une norme présentant un degré d'indétermination élevé n'est pas sans risques et, bien que l'interprétation qui pourra en être faite par les autorités administratives et les juges pourra permettre son application à une grande variété de situations, il est des cas de figure dans lesquels la complexité ou la spécifité rendront l'application d'une telle norme inefficace.

Le GDPR appartient à cette seconde catégorie de textes normatifs, en ce qu'il a vocation à être appliqué à une variété indéterminée de situations de traitement de données à caractère personnel. Pour ce faire, le législateur européen s'est appuyé sur le principe de neutralité technologique[171]. Ainsi, le GDPR s'appliquera à tout traitement de données à caractère personnel sans qu'il soit nécessaire de prendre en compte le ou les moyens techniques utilisés. De la sorte, les auteurs du GDPR ont souhaité créer une réglementation qui ne s'applique pas à « un outil technologique spécifique » afin d'éviter les risques « de désuétude des principes dès que la technologie sera dépassée ou abandonnée » et « d'inadaptabilité des règles énoncées aux nouvelles technologies »[172].

Bien que présentant certains avantages, le principe de neutralité technologique nous paraît toutefois dépassé lorsque la réglementation qui en

[170] E. Palmerini, « The interplay between law and technology, or the Robolaw project in context », *Law and Technology, the Challenge of Regulating Technological Development* (E. Palmerini et E. Stradella dir.), Pisa, Pisa University Press, 2013, pp. 16-17.

[171] Voy. GDPR, consid. 13 : « La protection des personnes devrait être neutre sur le plan technologique et ne pas dépendre des techniques utilisées, sous peine de créer de graves risques de contournement ».

[172] C. De Terwangne, « La modernisation de la Convention 108 du Conseil de l'Europe », *Le développement du droit européen en matière de protection des données*, Bâle, Schulthess, 2012, p. 27.

est inspirée se trouve confrontée à une technologie de rupture[173]. Nous l'avons vu, de par leurs capacités inédites à la collecte constante et « invisible » de grandes quantités de données à caractère personnel, leur capacité de mouvement..., les robots mettent parfois à mal les règlementations existantes ou en tout cas leur efficacité (limite du champ d'application du GDPR, obligations reposant potentiellement sur l'utilisateur du robot et non sur le fabricant, modalités d'exercice des droits des personnes concernées...).

75. Rationalités divergentes – Deuxièmement, la régulation d'une technologie émergente doit se trouver au carrefour entre deux rationalités différentes. Ces deux rationalités sont, d'une part, celle de voir la technologie fonctionner et, d'autre part, celle de protéger la société face aux éventuels dangers présentés par cette technologie.

Cette différence de rationalité est la source de postures différentes relatives aux données collectées par les robots. Quand le concepteur voit le traitement de données personnelles comme un moyen d'assurer un fonctionnement correct et satisfaisant pour les utilisateurs, le régulateur voit ce traitement comme une potentielle atteinte à la vie privée des citoyens[174].

Pour le législateur, trouver le point de rencontre entre ces deux rationalités consiste à veiller à la protection de la vie privée des utilisateurs tout en prenant en considération les bienfaits pour la société que peuvent amener la conception et la mise sur le marché de robots.

76. Perspectives – Le Comité européen de protection des données pourrait, dans un avis qui concernerait la manière d'appliquer le GDPR aux robots, tenter de trouver cet équilibre.

Toutefois, cet avis ne pourra probablement pas répondre à certains problèmes posés spécifiquement par les robots, c'est pourquoi nous serions plus favorables à une législation particulière pour ces derniers.

Parmi les autres solutions envisageables pour concilier ces deux visions opposées, l'on pourrait également imaginer la mise en place de codes de conduite (incluant notamment le respect du principe de *privacy by design*) auxquels les producteurs de robots devraient souscrire afin de pouvoir être autorisés à commercialiser leurs produits sur le territoire européen.

---

173 I. Kerr et K. Szilagyi, « Asleep at the switch ? How killer robots become a force multiplier of military necessity », *Robot Law* (R. Calo, A. M. Froomkin et I. Kerr dir.), Cheltenham, Edward Elgar, 2016, pp. 348-349.

174 C. Lutz et A. Tamò, « RoboCode-Ethicists – Privacy-friendly robots, an ethical responsibility of engineers ? », *op. cit.*, pp. 6-7.